Brownian Motion and *Random* Prime Factorization

Kendrick Tang

March 5, 2013

Contents

1 Introduction

This paper will reflect the material covered in Patrick Billingsley's *Prime Numbers and Brownian Motion* paper from 1973 [1]. First I will develop some concepts of Brownian motion and introduce the Wiener measure for subsets of the set of continuous functions which map the unit interval to the real line. Afterwards I will introduce a prime-factorization counting function and some properties. In the final section of my paper, the two seemingly separate ideas will be tied together: I will construct a random path from the integers using the prime-factorization counting function and use tools explained in the previous sections to modify the path to model Brownian motion. Then using a probability limit, I will conclude several interesting properties of the prime factorization of numbers.

2 Brownian Motion

2.1 Developing Brownian Motion

Brownian motion is a mathematical model of a particle that displays inherently irregular and random movements. In this paper I will only be focusing on one dimensional Brownian motion. It is in this section where I introduce and define some necessary conditions for Brownian motion and notation, as well as the Wiener measure. However, I must first begin by defining measure spaces and Borel sigma algebras.

2.1.1 Measure Spaces and Borel Sigma-Algebras

The following material does not need to be fully understood for the reader to understand the rest of the paper. It is, however, an introduction to measure theory and borel sigma algebras which are both deeply involved in the constraints of the big theorems of this paper. This section can be skipped by the reader, and used as a reference when measure theory and borel sets are mentioned in the later parts of this paper.

Definition 2.1. A measurable space defined by a large sample space Ω, a subset of Ω, B, and is coupled with a measure, μ to form a measure space. A measure space is notated by (Ω, B, μ).

In this paper we will be focusing on the set of continuous functions that map the unit interval to the real line C_0, and sigma-algebras of C_0, specifically the Borel sigma-algebra.

Definition 2.2. A sigma-algebra (σ-algebra) is a collection of subsets of the sample space that contains the empty set, is closed under countable unions, and is closed under complements [2].

The largest sigma-algebra of Ω is the powerset of Ω, and the smallest sigma-algebra is $\{\varnothing, \Omega\}$ [2]. For this paper we will only consider the Borel sigma-algebra:

Definition 2.3. The Borel sigma-algebra on Ω is the smallest sigma-algebra containing all open sets of Ω, and a Borel set is an element of the Borel sigma-algebra [2].

The measure in a measure space can be any kind of measure. In this paper we will only consider the Wiener measure (described in 2.1.3), which is a probalility measure, so we refer to our measure space as a probability space. Thus, we can write the measure space this paper focuses on as

$$(C_0[0,1], A, P_1)$$

where $C_0[0,1]$ is the set of continuous functions on the unit interval, A is a subset of $C_0[0,1]$, and P_1 the Wiener measure of Borel sets on $C_0[0,1]$.

However, to form a sigma algebra on $C_0[0,1]$ we must be able to define an open set. Thus, we define the metric for paths in $C_0[0,1]$ to be

$$d(f,g) = \max |f(x) - g(x)|, f, g \in C_0[0,1]$$

the maximum vertical displacement of two functions in $C_0[0,1]$. A set S is open if for every x in S, there is a neighborhood around x that is completely contained in S. In other words, for each x in S, there is an ϵ greater than 0 so that all y for which $d(x,y) < \epsilon$ are contained in S.

Again, these Borel sets are not of great importance to understand the material in this paper, but are important to keep in mind because of some constraints on the Wiener measure which will be described later in the paper.

2.1.2 A Collection of Continuous Paths

Consider the function $x(t) : [0,T] \mapsto \mathbb{R}$ that represents the vertical position of a particle that begins at the origin: $x(0) = 0$. At each infinitesimal time interval, the particle will either take an infinitesimal step up or down. Thus, $x(t) \in C_0[0,T]$ where $C_0[0,T]$ is the set of all continuous functions that map $[0,T]$ to the real line and satisfy $x(0) = 0$. For the majority of this paper, I will only either be working with the set of functions $C_0[0,1]$ (continuous functions mapping the unit interval to the real line), or a special mapping of functions in $C_0[0,T]$ to $C_0[0,1]$ defined later in §2.1.5.

2.1.3 A Short Introduction to Wiener Measure

The measureable space $C_0[0,1]$ is of little interest in this paper. Instead we are interested in subsets A and the probability mesaure to derive interesting properties of A. This measure, the Wiener measure $P_T(A)$, determines the probability that a function $x \in C_0[0,T]$ is in A. For example, if $A = \{x(t) : x(t) < 0, \forall t \in [0,T]\}$, is the set of functions which always have negative displacement, then $P_T(A)$ would be the probability that a function randomly picked from $C_0(0,T)$ will also be in A. At this point, the reader should note that it is not always possible to define $P_T(A)$ for all subsets of $C[0,T]$. However, originally proven by Norbert Wiener in 1923 [1], the existance of $P_T(A)$ does exist for all Borel sets (see 2.3). Also note that deriving the Wiener measure of a subset A is beyond the scope of this paper; we will only be examining the Wiener measure of three different subsets.

2.1.4 Three Defining Properties of Browning Motion

Using the Wiener measure for a specific subset of C_0, I will define two of the criteria for Brownian motion. Consider the event

$$A = [x : \alpha \leq x(t) \leq \beta], \tag{2.1}$$

the set of functions where the particle travels through the vertical *gate* $[\alpha, \beta]$ at time t. Note that the only restriction on α, β is that $\alpha < \beta$. The Wiener measure of this event (a relationship taken for granted in this paper) is defined in [1] to be

$$P_T[x : \alpha \leq x(t) \leq \beta] = \frac{1}{\sqrt{2\pi t}} \int_\alpha^\beta e^{-u^2/2t} du. \tag{2.2}$$

Note that (2.2) is the integral of a gaussian with mean 0 and variance t. These will be the first two defining properties of Brownian motion. These two properties reflect non-drift (since there is an equal chance of moving up or down) and the particle's tendency to wander away from the origin. We will expect anything that exhibits Brownian motion to satisfy this property.

The third property of Brownian motion is independence. Particles in Brownian motion move randomly, which means the direction a particle moves in one time interval is completely independent of how the particle moves in another time interval. Consider $t < t' < s < s'$. If A is the subset of functions with property M defined on $[t, t']$ and B the subset of functions with another property N on $[s, s']$ then

$$P_T(A \cap B) = P_T(A) P_T(B). \tag{2.3}$$

The probability that x is in the intersection of A and B is the product of the probability of $x \in A$ and the probability of $x \in B$ because the probability of each event happening is independent of each other [1]. This can be generalized to multiple events:

Lemma 2.1. *If $A_1, ...A_n$ are sets of functions that satisfy properties for $t \in \tau_1 \subset [0, T]$ where $\tau_i \cap \tau_j = \varnothing$ for all i, j then*

$$P_T(A_1 \cap A_2 \cap ... \cap A_n) = P_T(A_1) P_T(A_2) ... P_T(A_n). \tag{2.4}$$

Proof. Since $A_1 \cup A_2 \cup A_3 = A_1 \cup (A_2 \cup A_3)$,

$$P_T(A_1 \cup (A_2 \cup A_3)) = P_T(A_1) P_T(A_2 \cup A_3)$$

and by (2.3),

$$P_T(A_1 \cup A_2 \cup A_3) = P_T(A_1) P_T(A_2) P_T(A_3).$$

Continue by induction to show (2.4) $\square$

In this paper, a particle is in Brownian motion if it satisfies the three properties restated below for the reader's convenience:

- For event (2.1), the Wiener measure must follow the distribution of a gaussian with mean zero
- and variance t.
- Events over disjoint time intervals must be independent of each other.

2.1.5 A Mapping From $C_0[0,T]$ to $C_0[0,1]$

In this section I define a mapping $C_0[0,T]$ to $C_0[0,1]$ which also preserves Bronian motion. Given a particle's path $x(t) \in C_0[0,T]$, speed up the argument by T and shrink the amplitude by $1/\sqrt{T}$:

$$y(t) = \frac{1}{\sqrt{T}} x(tT), t \in [0,1]. \tag{2.5}$$

Theorem 2.2. *If $y(t)$ is defined by (2.5) then $y(t) \in C_0[0,1]$ and $y(t)$ will exhibit Brownian motion (as described in* §2.1.4*) [1].*

Proof. Since $x(t)$ describes Brownian motion, the Wiener measure of $x(t)$ through the gate $[\alpha, \beta]$ at time t will be defined by a gaussian with mean 0 and variance t. By changing the time scale, $x(tT)$ will have a similar Wiener measure, with mean 0, but variance now tT:

$$P_T[x(tT) : \alpha \leq x(tT) \leq \beta] = \frac{1}{\sqrt{2\pi t}} \int_\alpha^\beta e^{-u^2/2tT} du.$$

By rescaling the random variable $x(t)$ the gaussian will change as follows: the mean will change by the scaling factor, and variance by the square of the scaling factor. Thus the mean remains zero, but the variance will be reduced to t since $tT\left(\frac{1}{\sqrt{T}}\right)^2 = t$. Furthermore, indepedent events will remain independent through the uniform time and displacement scaling. Therefore, the mapping maps $C_0[0,T]$ to $C_0[0,1]$ and preserves Brownian motion. □

This mapping has an interesting consequence:

Theorem 2.3. *For any $\epsilon > 0$, $K > 0$, define A to be functions with at least one chord with slope exceeding K. Then $P_1(A) > 1 - \epsilon$ [1].*

Proof. Let $\epsilon > 0$ b First begin with $x(t) \in C_0[0,T]$. Choose T large enough so with probability larger than $1-\epsilon$, $x(t)$ will have slope larger than 1. This *event* isn't too strange and unfathomable that given enough time, it is guaranteed that $x(t)$ will produce this given enough time. Also make sure T is larger than K^2. Now $x(t)$ is a function with slope at least 1 and belongs in $C_0[0,T], T > K^2$. Now map $x(t)$ to $y(t)$ with (2.5). By shrinking the time scale, the slope is increased from 1 to T. By shrinking the vertical scale by $1/\sqrt{T}$ the slope is then reduced to $T/\sqrt{T} > K^2/K = K$. □

I will now present, but not prove, some corollaries of 2.3, which are mentioned in [1]:

Corollary 2.4. *Since ϵ and K were chosen arbitrarily, with probability 1 a randomly picked function from $C_0[0,1]$ will have at least one point of unbounded positive or negative variation.*

Corollary 2.5. *It follows that the chords with unbounded slopes are infinitely dense in functions from $C_0[0,1]$. This means with probability 1, a function from $C_0[0,1]$ will be nowhere differentiable.*

2.2 Applying the Wiener Measure

In this section I will provide some well known Wiener measures and apply them to produce some interesting probabilities. I will come back to these measures when examining prime number factorization in the last section of this paper.

2.2.1 Distribution of the Greatest Positive Excursion

Consider the set of functions A so that $x \in A$ if $x(t), t \in [0,1]$ exceeds some α. Since $x(1) \geq \alpha$ and $x(1) < \alpha$ are mutually exclusive events, one or the other is guaranteed to happen which means

$$\begin{aligned} P_1[x : \max x(t) \geq \alpha] = &P_1[x : \max x(t) \geq \alpha \text{ and } x(1) \geq \alpha] \\ &+ P_1[x : \max x(t) \geq \alpha \text{ and } x(1) < \alpha]. \end{aligned}$$

Since the particle has no drift, after arriving at height α the particle has an equal probability of continuing to increase, or to decrease. Thus, the two events are equivalent and we can combine the probabilities into one:

$$P_1[x : \max x(t) \geq \alpha] = 2P_1[x : \max x(t) \geq \alpha \text{ and } x(1) \geq \alpha].$$

At this point, the second restriction on x is redundant: if $x(1)$ exceeds α then the original restriction is automatically satisfied. So finally,

$$P_1[x : \max x(t) \geq \alpha] = 2P_1[x : x(1) \geq \alpha]$$

which is (2.1) where $t = 1$ and $\beta = \infty$. Thus, using (2.2)

$$P_1[x : \max x(t) \geq \alpha] = \frac{2}{\sqrt{2\pi}} \int_{\alpha}^{\infty} e^{-u^2/2} du \tag{2.6}$$

which is the Wiener measure of all functions which exceed α at some $t \in [0,1]$.

2.2.2 Paul Levy's Arcsine Law

Let $x(t) \in C_0[0,1]$ and define the set S to be the set of points t so that $x(t) > 0$. Then the Lebesgue measure of S is written as $\mu_{\mathcal{L}}(\{t : x(t) > 0\})$ the total amount of time x is positive. Now consider the set of functions

$$x(t) : \alpha \leq \mu_{\mathcal{L}}(\{t : x(t) > 0\}) \geq \beta. \tag{2.7}$$

The Wiener measure of this subset of $C_0[0,1]$ is given in [1] as

$$P_1(A) = \frac{1}{\pi}\int_{\alpha}^{\beta} \frac{du}{\sqrt{u(1-u)}}.$$

This is a u-shaped distribution, which means for a fixed $\beta - \alpha$ gate, the probability is lowest for α, β near 0.5 and highest for α, β near 0 and 1. Also, the graph is symmetric so the probability of passing the gate $[\alpha, \beta]$ is the same as passing the gate $[1-\beta, 1-\alpha]$.

2.2.3 The Gambler's Fortune

In this section I will construct continuous Brownian motion from a discreet random walk and apply the previous Wiener measures to provide some interesting probabilities.

Consider discreet random walks in one dimension. A particle begins at the origin, and at every integer time value, it takes either one step forward or one step backwards. If we connect the total displacement at each integer time value with straight lines to produce a continuous function, then this particle's path belongs in $C_0[0,T]$. This motion, satisfies the two properties of Brownian motion described in §2.1.4: at each step the mean is

$$(1)(0.5) + (-1)(0.5) = 0$$

and the variance

$$(1)^2(0.5) + (-1)^2(0.5) = 1$$

and the displacement at each step is surely independent. Let $y(t)$ be the polygonal path defined by the random walk. The linearity of the paths between each integer time interval is not something we want in Brownian motion so to remove the polygonal blemish in $y(t)$ and preserve the properties we want, take T to infinty and apply (2.5). Since we are contracting the time intervals by $1/T$, as $T \to \infty$ the time intevals become infinitesimal, and we approach continuous Brownian motion. Now consider a Gambler who's net fortune is mapped in this random walk. At each hand or game he can win or lose one dollar. By applying (2.5) to a random walk and take T to infinity, the probability measure approaches the Wiener measure [1]:

Corollary 2.6. *If $y(t)$ is defined by random walk, $x(t)$ the result of applying (2.5) to $y(t)$, and A any subset of $C_0[0,1]$ then*

$$Probability(x(t) \in A) \to P_1(A) \text{ as } T \to \infty.$$

Consider $A = [x : \alpha \leq x(1) \leq \beta]$. If $x(1) = h$ then $y(T) = h/\sqrt{T}$ by (2.5). So by corollary 2.6 and (2.2)

$$\text{Probability}\left[\alpha \leq \frac{y(T)}{\sqrt{T}} \leq \beta\right] \to \frac{1}{\sqrt{2\pi}}\int_{\alpha}^{\beta} e^{-u^2/2} \text{ as } T \to \infty.$$

The following three examples are applications of the various Wiener measures applied to a Gambler who plays 100 hands:

- Consider (2.1) and let $-\alpha = \beta = 0.9$, the Wiener measure evaluates to about 0.6. If the Gambler plays 100 hands ($T = 100$) then the Gambler has a 60% chance of ending within $0.9\sqrt{100} = 9$ dollars of what the Gambler started with.

- Now consider (2.6). The history of the Gambler's fortune belongs in A if at any point during the night the Gambler's net winnings was larger than $\alpha\sqrt{T}$. If $\alpha = 1.7$, the Wiener measure is about 0.1 and again if we set $T = 100$ then the Gambler will have a 10% chance that at some point during the Gambler's 100 hands the Gambler will have 17 dollars more than what the Gambler started with.

- Now consider (2.7). We can estimate the probability that the Gambler's net fortune will be positive for a certain percentage of time. If $\alpha = 0.45, \beta = 0.55$ then the Wiener measure is about 6% (the Gambler has a 6% chance of being positive for around half the night). Again, noting the interesting feature of Paul Levy's Arcsine Law, if $\alpha = 0.9, \beta = 1$ then the Wiener measure is near 20%. By the symmetry of the arcsine curve, the same is true for $\alpha = 0, \beta = 0.1$. Thus, the Gambler has a 20% chance of being positive for 90% of the night, but also only for 10% of the night (meaning he has a 20% chance of being negative for 90% of the very same night).

While for the three A's above, the probability limit converges to the Wiener measure, this is not always the case. The proof is beyond the scope of this paper, but it is important to note that the convergence is only the case for every Borel set (see 2.3) A where for the boundary of A, denoted by ∂A, satisfies $P_1(\partial A) = 0$ [1].

3 A Different Prime Counting Function

3.1 Defining the Function

Definition 3.1. I will say that n divides m if $\lfloor m/n \rfloor$ is zero and denote this with $n|m$. Otherwise, n does not divide m, which we will be denote with $n \not| m$.

Let

$$\delta_p(n) = \begin{cases} 1 & p \mid n \\ 0 & p \nmid n \end{cases}$$

and define

$$f(n) = \sum_{p \text{ prime}} \delta_p(n).$$

In other words, f counts the number of distinct primes in the factorization of n. This function increases very very slowly. In fact, f equals 2 first at $n = 6$, 3 at $n = 30$ and 4 at $n = 210$. Despite its growth rate, there are infinitely many primes so f must eventually approach infinity.

3.2 Primes and Probability

We can define

$$\mathbf{P}_N(S) = \frac{1}{N} * \nu\{n : n \in [1, N] \text{ and } n \in S\}$$

where ν measures the number of integers in a set. This means $\mathbf{P}_N(S)$ is the ratio of integers in $[1, N]$ that are also in S. For example, if S is the set of even numbers, $\mathbf{P}_{10}(S) = 5/10 = 1/2$. Now consider $\mathbf{P}_N(n : \alpha \leq f(n) \leq \beta)$. This is the probability that a andomly picked integer between 1 and N will have between α and β primes in its factorization.

The number of multiples of p up to N is $\lfloor N/p \rfloor$. For example, if $N = 50$ and $p = 7$ then there are exactly $\lfloor 50/7 \rfloor = 7$ numbers between 1 and 50 that have 7 in its factorization. Thus, the probability that $p|n$, or that $\delta_p(n) = 1$, is

$$\mathbf{P}_N[n : p|n] = \frac{1}{N}\left\lfloor \frac{N}{p} \right\rfloor \approx \frac{1}{p} \text{ for large } N[1]. \tag{3.1}$$

This approximation is good for *very* large N since $|\lfloor N/p \rfloor - N/p| < 1$ and as $N \to \infty$ the difference between the floor of the quotient and regular division gets proportionally small.

Now consider two relatively prime numbers a and b (they share no prime factors). Then $a|n$ and $b|n$ if and only if $ab|n$. Since two prime numbers are automatically relatively prime, we can deduce with (3.1) that

$$\mathbf{P}_N(n : p|n \text{ and } q|n) = \mathbf{P}_N(n : qp|n) = \frac{1}{N}\left\lfloor \frac{N}{pq} \right\rfloor \approx \frac{1}{p} \cdot \frac{1}{q}$$

Since $\frac{1}{p} \approx \mathbf{P}_N(n : p|n)$ and $\frac{1}{q} \approx \mathbf{P}_N(n : q|n)$ it is clear that prime factorization between two primes are approximately independent:

$$\mathbf{P}_N(n : p|n \text{ and } q|n) \approx \mathbf{P}_N(n : p|n)\mathbf{P}_N(n : q|n) \tag{3.2}$$

This theorem generalizes as follows:

Theorem 3.1. *If $p_1, ...p_k$ are k distinct primes, then*

$$P_N(n : p_1|n, p_2|n, ... \text{ and } p_k|n) = \boldsymbol{P}_N(n : p_1|n)...\boldsymbol{P}_N(n : p_k|n).$$

Proof. If $p_1, ...p_k$ are k distinct primes then p_1 is relatively prime to $\Pi_{j=2}^{k} p_j$ which, by induction produces the theorem. □

4 Brownian Motion and Primes

How can we relate the prime counting function described in the previous section and Brownian motion? First I will introduce a useful approximation and then outline how the random displacement will take be defined. The output of this will satisfy independence due to Theorem 3.1 but due to the rareness of primes and the slow growth rate of $f(n)$ there will be drift and variance problems involved.

4.1 A Very Useful Approximation

Theorem 4.1. *The approximation: If $q \in$ primes then for large enough p,*

$$\sum_{q \le p} \frac{1}{q} \approx \log \log p. \tag{4.1}$$

Proof. This proof is outline in [3], and is reproduced below: We first need four inequalities.

Lemma 4.2.

$$\sum_{k=1}^{n} \frac{1}{k^2} < 5/3$$

Proof. The sum converges to $\pi^2/6$ which is less than $5/3$. □

Lemma 4.3.

$$1 + x < e^x \text{ for all } x > 0.$$

Proof. When $x = 1$ both sides are equal to 1, and e^x grows much faster than x. □

Lemma 4.4.

$$\log(n+1) < \sum_{i=1}^{n} \frac{1}{i}.$$

Proof. The log term can be written as $\int_1^{n+1} \frac{dx}{x}$ which can then be split into a sum of integrals $\sum_{i=1}^{n} \int_1^{i+1} \frac{dx}{x}$. Since $1/x$ is a decreasing function, $1/i$ is the maximum value for each interval which means the sum of integrals is less than $\sum_{i=1}^{n} \frac{1}{i}$. □

Lemma 4.5.

$$\sum_{i=1}^{n} \frac{1}{i} \le \prod_{p \le n} \left(1 + \frac{1}{p}\right) \sum_{k=1}^{n} \frac{1}{k^2}$$

Proof. Each integer can be written as a product of a square free integer and an integer, that is $i = k^2 p$ or $\frac{1}{i} = \frac{1}{k^2}\frac{1}{p}$, where $i, k, p \in \mathbb{R}$ and $p \le i$. Also $\frac{1}{p} \le \prod \frac{p+1}{p}$ because each term on the right side is larger than 1. □

So

$$\log(n+1) \le \prod_{p \le n} \left(1 + \frac{1}{p}\right) \sum_{k=1}^{n} \frac{1}{k^2} \le \prod_{p \le n} \left(\exp\left(\frac{1}{p}\right)\right) \frac{5}{3} = \exp\left(\sum_{p \le n} \frac{1}{p}\right) \frac{5}{3}$$

which means that

$$\log[\log(n+1)3/5] \le \sum_{p \le n} \frac{1}{p},$$

or that

$$\log\log(n+1) - \log(5/3) \leq \sum_{p \leq n+1} \frac{1}{p} - \frac{1}{n+1}.$$

This can be rearranged to be

$$\log\log(n+1) - \sum_{p \leq n+1} \frac{1}{p} \leq \log\frac{5}{3} - \frac{1}{n+1}$$

and as n goes to infinity, the difference is bounded and pretty small, so for large enough n this is a good approximation. □

The time passed at prime p is given by $\sum_{q \leq p} 1/q$ and current height given by $\sum_{q \leq p}(\delta_q(n) - 1/q)$. By the approximation (4.1) we can say that the time passed is about $\log\log p$ and the height about $\sum_{q \leq p}(\delta_q(n) - \log\log p)$.

4.2 Constructing and Correcting the Path

4.2.1 Constructing the path

Let N be given. Randomly choose n from $[1, N]$ and begin the path at 0. At each prime (starting at $p = 2$), if $p|n$ then move up one step, else move one step down. Then proceed to the next prime and repeat.

While it seems like this path will be predetermined once n has been picked, there is an inherent randomness in choosing n. It is from this randomness the Brownian motion will be derived. Imagine playing this game with a mysterious helper who picks the n and does not immediately reveal the number. It is only at each prime step whether or not $p|n$ and which way to move is revealed. With the help of the mysterious player, it is clear that the that will truly be random.

A problem arises from the fact that most primes will not divide the number. Thus, there will be an intense drift in the negative direction since there will be many negative steps between each positive step. In fact, by (3.1) as p goes to infinity, $1/p$ goes to 0 which means the chances of p dividing n goes to 0.

4.2.2 Correcting the Drift

To correct the drift we change the magnitude of the steps. Everytime we move in the positive direction, move forward by $1 - \frac{1}{p}$, and everytime we move in the negative direction, move backwards by $\frac{1}{p}$. These changes in the steps taken will reduce the mean to be closer to 0 and dampen the drift.

Proof.

$$\begin{aligned}\left(1-\frac{1}{p}\right)\mathbf{P}_N(n : p|n) + \left(-\frac{1}{p}\right)\mathbf{P}_N(n : p \nmid n) &\approx \left(1-\frac{1}{p}\right)\left(\frac{1}{p}\right) + \left(-\frac{1}{p}\right)\left(1-\frac{1}{p}\right) \\ &= \left(1-\frac{1}{p}\right)\left(\frac{1}{p}\right) - \left(\frac{1}{p}\right)\left(1-\frac{1}{p}\right) \\ &= 0.\end{aligned}$$

□

4.2.3 Correcting the Variance

With the mean fixed, there is now a problem with the variance:

$$\begin{aligned}\left(1-\frac{1}{p}\right)^2 \mathbf{P}_N(n:p|n)+\left(-\frac{1}{p}\right)^2 \mathbf{P}_N(n:p\not| n) &\approx \left(1-\frac{1}{p}\right)^2\left(\frac{1}{p}\right)+\left(-\frac{1}{p}\right)^2\left(1-\frac{1}{p}\right)\\ &=\left(1-\frac{2}{p}+\frac{1}{p^2}\right)\left(\frac{1}{p}\right)+\left(\frac{1}{p^2}-\frac{1}{p^3}\right)\\ &=\left(\frac{1}{p}-\frac{2}{p^2}+\frac{1}{p^3}\right)+\left(\frac{1}{p^2}-\frac{1}{p^3}\right)\\ &=\frac{1}{p}\left(1-\frac{1}{p}\right)\end{aligned}$$

As p gets large, the variance goes to $1/p$ which gets very very small. This is a problem because this implies that the Brownian motion will have very little vertical displacement over each step after a large enough amount of steps. To resolve this problem, we need to change the amount of time spent at each step. The correct thing to do is to spend only $1/p$ time units at each prime p.

Proof. Since the vertical variance at each prime is about $1/p$, and we are spending $1/p$ time at each step, the total vertical variance is approximately $\sum_{q\le p, q \text{ prime}} 1/q$, which is the same as the variance of time. Thus, horizontal and vertical variances are proportional and we can say that the variance is approximately t. $\square$

4.2.4 Correcting the Path Polygonality

If we are checking numbers from $[1, N]$, at the last prime N the total amount of time spent will be $\sum_{q\le N} 1/q \approx \log\log N$. Let $T = \log\log N$. At this point we are faced with the same problem we had with the random walk: the steps are too polygonal! To correct this, we do the same steps as before: send T to infinity and apply (2.5). After rescaling, the path is now part of $C_0[0, 1]$, has mean 0, variance t and event independence. Sending T to infinity will correct the polygonal shape of the path, allowing the path to approach continuous Brownian motion.

After transforming the path, time t will transform to time $\log\log p/\log\log N$ and the vertical scale will be contracted to

$$\frac{\sum_{q\le p}\left(\delta_q(n)-\log\log p\right)}{\sqrt{\log\log N}}.$$

4.3 Properties of Integers using Prime Factorization

In this section I will make use of a useful approximation and the paths constructed in the previous section to conclude some interesting properties of n. These paths, denoted by $\text{path}_N(n)$ since they are dependent on both N and

n, are in $C_0[0,1]$. The probability that $\text{path}_N(n) \in A$ where A is a subset of $C_0[0,1]$ is

$$\mathbf{P}_N[n : \text{path}_N(n) \in A]$$

and, similarly to corollary 2.6:

Theorem 4.6. *[1] If A is a Borel subset of $C_0[0,1]$ satisfying $P_1(\partial A) = 0$ then*

$$\boldsymbol{P}_N[n : path_N(n) \in A] \to P_1(A) \text{ as } N \to \infty \tag{4.2}$$

The proof of this theorem goes beyond my ability... But, like the approximations with the Gambler's fortune, we can determine some probabilitistic properties of n.

I will now use this limit to consider the following three sets of $x \in C_0$ so that

a. the final value of x lies between α and β, so that

$$P_1 = \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta e^{-u^2/2} du;$$

b. the max value of x is greater than α, so that

$$P_1 = \frac{2}{\sqrt{2\pi}} \int_\alpha^\infty e^{-u^2/2} du;$$

c. and where the time with which x is positive is between α and β, so that

$$P_1 = \frac{1}{\pi} \int_\alpha^\beta \frac{du}{\sqrt{u(1-u)}}.$$

Example 4.1. Consider (a). If $-\alpha = \beta = 0.9$ and $N = 10^{70}$ so $\log\log N \approx 5$, then the probability that the path is in the set approaches the Wiener measure, which evaluates to 0.6. Thus, about 60% of $n \leq 10^{70}$ have 3 to 7 prime factors.

Example 4.2.

Definition 4.1. The apparent "compositeness" of n up to a prime p is

$$\left[\sum_{q \leq p} \delta_q(n)\right] - \log\log p.$$

The larger this is, the more composite n seems to be at a prime p and the smaller this is, the more prime-like n seems to be.

So the max apparent compositeness of n is

$$\max_{p \leq N} \left[\left(\sum_{q \leq p} \delta_q(n)\right) - \log\log p\right] = \left[\max_{p \leq N} path_N(n)\right] \sqrt{\log\log N}.$$

If we consider (b) and let $\alpha = 1.7, N = 10^{70}$ then the probability that $Path_N(n)$ has max value larger than 1.7 approaches the Wiener measure in (b), which evaluates to 0.1. This means about 10% of n less than 10^{70} has a max apparent compositeness of about 3.8.

Example 4.3.

Definition 4.2. A number n is excessive at a prime p if

$$\sum_{q \leq p} \delta_q(n) > \log\log p.$$

That is, the number n is more composite than the average number up to p.

It follows from the definition that a number n is excessive at p if $path_N(n) > 0$ at a p. The total amount of time with which $path_N(n)$ is positive is

$$\frac{1}{\log\log N} \sum \left[\frac{1}{p} : p \leq N \text{ and } \sum_{q \leq p} \delta_q(n) > \log\log p \right].$$

The first quotient is the factor time is scaled by when correcting the path. Since we spend $1/p$ of unscaled time at each prime, and are considering only the p where n is excessive at p, the second part of the product is the sum of $1/p$ where n is excessive at p. If we compare this to (c), again with $N = 10^{70}$, we can observe that

- 20% of $n < N$ are excessive more than 90% of the time [1],
- (by the same symmetry discussed in §2.2.3) 20% of $n < N$ are excessive less than only 10% of the time [1],
- and only about 6% of $n < N$ are excessive from 45% to 55% [1].

These three properties indicate that very few integers are undecidedly composite, that is, if a number is highly composite at some p (or very prime-like), it is very likely that the number will be highly composite (or very prime-like) for most other p.

If we consider

$$\varphi_N(n) = \# \left[p : p \leq N \text{ and } \sum_{q \leq p} \delta_q(n) > \log\log p \right],$$

so that $\varphi_N(n)$ is the number of primes up to N where n is excessive, and the ratio of φ. The ratio of $\varphi_N(n)$ and the regular prime counting function $\pi(N)$ is defined in [1] as:

Definition 4.3. $R_N(n) = \frac{\varphi_N(n)}{\pi(N)}$ is the ratio of primes where n is excessive over the total number of primes. (This is the number of p where n is excessive, normalized by the number of primes)

Theorem 4.7. *[1] Let $P(R > \alpha)$ be the probability that the ratio R is larger than α, $\alpha > 1$. The given an $\epsilon > 0$, there exists a K so when N is greater than K,*

$$|P(R < \epsilon) - 1/2| \leq \epsilon \textit{ and } |P(R > 1 - \epsilon) - 1/2| < \epsilon.$$

This theorem follows from the fact that most integers are either excessive at most primes, or not excessive at most primes. Taking N large enough, and normalizing by the prime counting function produces the theorem. In other words for large enough N, for about 50% of the time the ratio is at 0, and the rest of the time the ratio will be at 1. This means, almost explicitly, that all integers are either excessive at all primes or at none [1].

5 Conclusion

While this paper doesn't go into the details of find Wiener measures or the rigorous mathematics behind Brownian motion, I am still able to compute some interesting quantities, using only simple algebra, number theory and probability. These quantities are deeply related to properties of the integers and their relationship with the primes.

References

[1] Patrick Billingsley. Prime numbers and brownian motion. *The American Mathematical Monthly*, 80(10 (Dec.)):1099–1115, 1973.

[2] Maya R. Gupta. A measure theory tutorial (measure theory for dummies). Technical Report UWEETR-2006-0008, May 2006.

[3] Wikipedia. Divergence of the sum of the reciprocals of the primes — Wikipedia, the free encyclopedia, 2012. [Online; accessed 1-June-2012].