Arithmetical Functions and Dirichlet Series

October 1, 2019

Contents

1 Introduction

Analytical number theory relies on analytic arguments to deduce arithmetic facts. For example, by considering the density of primes in an arithmetic progression relative to the growth of all primes, one can prove Dirichlet's Theorem which asserts that any arithmetic progression contains infinitely many primes (See [2, §3.6]).

The main aim of this essay is to investigate some of the methods of analytic number theory. In order to demonstrate these, we will be motivated by these questions:

1. How many elements less than n are coprime to it?
2. How are the primes distributed?
3. What is the probability two (or more) random numbers are coprime?

The answer to 1 immediately defines an arithmetic functions for us, which we will come to soon.

The second question is an important topic due to its difficulty but is beyond the scope of this essay. The techniques used, however, can be applied to the study of this question.

The final question is interesting, but vague. We will not answer it strictly, but rather use the results we develop to find the limit as n tends to infinity of the probability of picking coprime numbers from the set $\{1, 2, ..., n-1, n\}$ in the chapter on Dirichlet Series. This is not strictly a probability, but rather a kind of density.

We will begin this essay by introducing the concept of an arithmetical function, and see that these behave as a ring when considered with the operation of Dirichlet multiplication. We will remark on other applications and move onto Dirichlet series. Here we will see how Dirichlet multiplication, as an operation on the arithmetic functions, interacts with multiplication of these series.

To end the essay, an answer to the third question will be given using the results obtained so far.

2 Arithmetic Functions

2.1 Examples

The proofs of the theorems in this section are mostly confined to the Appendix since they are technical and not very informative. We begin with the Euler Phi function, defined as follows:

Definition 2.1 (Euler Phi Function)**.** The function $\phi(n)$ counts the numbers less than n which are coprime to n. More concisely:

$$\phi(n) = \sum_{\substack{r<n \\ (r,n)=1}} 1$$

.

This satisfies some useful properties.

Lemma 2.1. For positive integers $m \geq 1, n \geq 1$

1. If $(m, n) = 1$ then $\phi(n)\phi(m) = \phi(nm)$.
2. $\phi(p^a) = p^a - p^{a-1}$ if p is a prime number and a is a positive integer.
3. $\sum_{d|n} \phi(d) = n$.

This lemma is proved (in various ways) in Algebra 2 and in Introduction To Number Theory.

Part 1. and 2. of the theorem us to obtain a more concrete formula for the Euler Phi function which until now has been defined in abstract terms.

Theorem 2.2. For $n \geq 1$

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where p ranges over primes dividing n.

The proof of this fact is obtained by use of the Fundamental Theorem of Arithmetic and parts 1. and 2. of the above lemma. See Appendix.

We note that there is an unproven conjecture concerning Euler's phi function.

Conjecture 1 (Carmichael's toitent function conjecture)**.** For every integer $n \geq 1$ there is a positive integer $m \neq n$ for which $\phi(n) = \phi(m)$

This was conjectured by Robert Carmichael in 1907. Carmichael provided a lower bound for a counterexample of 10^{37} and since then the bounds have increased to 10^{10^7}.[5]

We now consider the second interesting function, which we will soon see has a special role in the theory of arithmetical functions:

Definition 2.2 (Möbius Function)**.** If $n = \prod_{i=1}^{k} p_i^{\alpha_i}$

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1. \\ 0, & \text{if any } \alpha_i > 1. \\ (-1)^k, & \text{if } \alpha_i = 1 \text{ for } i = 1, 2, ..., k. \end{cases}$$

Theorem 2.3. The Möbius Function has the following properties:

1. $\mu(n)\mu(m) = \mu(mn)$ if m and n are coprime.
2. $$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1. \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

Despite these nice properties, the definition for μ seems strange, almost contrived, in contrast to the more natural definitions that have come before. We shall see why it is so useful in the chapter on Dirichlet Multiplication, in which there is a much shorter proof of the following theorem:

Theorem 2.4.

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

.

Here we will prove this theorem, since it is useful to compare with its generalisation:

Proof. Let us suppose n has k distinct prime factors.

By Theorem 2.2 we have the product form of ϕ.

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

.

By expanding the product we obtain:

$$\prod_{p|n} \left(1 - \frac{1}{p}\right) = \sum_{p|n} \frac{-1}{p} + \sum_{p_i<p_j} \frac{1}{p_i p_j} + ... = \sum_{r=1}^{k} \sum_{p_{i_1}<...<p_{i_r}} \frac{(-1)^r}{p_{i_1} p_{i_2} ... p_{i_r}}$$

.

Here the p_{i_j} range over all the primes dividing n. The strict inequalities are to ensure no primes are repeated. The claim is now that this sum is the same as $\sum_{d|n} \mu(d)\frac{1}{d}$.

Remembering the definition of μ we see that the only non-zero terms in this sum are precisely those whose denominator is a square-free divisor of n, with signs dependent μ. The squrefree divisors are obtained by taking every possible product of the distinct primes dividing n and the sign of each term are those given by evaluating μ of that product. And so the previous expression is exactly $\sum_{d|n} \mu(d)\frac{1}{d}$.

To conclude:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \sum_{d|n} \mu(d) \frac{1}{d}$$

□

Note, here we have proved this theorem using the product form of $\phi(n)$. In[2], Tom M. Apostle proves this relationship first and then uses it to deduce the product form.

Also notice that obtaining the product form of ϕ was possible due to the first property in Lemma 2,1, that $\phi(mn) = \phi(n)\phi(m)$ for coprime m and n. We shall give a name to this property now:

Definition 2.3. An arithmetical function f is multiplicative if f is not identically 0 and for every pair of naturals m and n such that $(m, n) = 1$ we have: $f(mn) = f(m)f(n)$.
Aditionally, if $f(mn) = f(m)f(n)$ for every pair of naturals m and n then f is completely multiplicative.

We have already shown that μ and ϕ are multiplicative. Neither is completely multiplicative. If m an n are both square free but share a prime then $\mu(mn) = 0$, and $\phi(2) = 1$,$\phi(4) = 2$ but $\phi(8) = 4$.

In general, the property of being multiplicative allows us to obtain product formulas. Not only this, but multiplicative functions are special since they have inverses under the (yet to be defined) operation of Dirichlet multiplication.

Before moving on, we shall state a few theorems about multiplicative functions:

Theorem 2.5. Given an arithmetical function f:

a) If f is multiplicative then, $f(1) = 1$.

b) f is multiplicative if and only if $f(p_1^{a_1}p_2^{a_2}...p_r^{a_r}) = f(p_1^{a_1})f(p_2^{a_2})...f(p_r^{a_r})$ where the p_i are prime numbers and a_i are positive integer.

c) f is completely multiplicative if and only if $f(p^a) = f(p)^a$ for all prime p and integers $a \geq 1$.

These proofs are are given in the Appendix.

2.2 Dirichlet Multiplication

To end this section, we will define Dirichlet multiplication and show that the set of arithmetic functions together with the operations addition and Dirichlet multiplication form a commutative ring.

Definition 2.4. The Dirichlet product (or convolution) of two arithmetical functions f and g is defined to be $\sum_{d|n} f(d)g(\frac{n}{d})$ and denoted $f * g$.

So far we have seen a few Dirichlet products already. Here they are again:

1. $N = \phi * u$.
2. $\phi = \mu * n$.
3. $I = \mu * u$.

Where I is 1 for $n = 1$ and 0 otherwise, u is function that is constantly 1, and N is the arithmetic function that sends n to n. We do not call it the identity function to avoid confusion since it is not the identity under the operation of Dirichlet multiplication.

Theorem 2.6. The set of arithmetical functions with Dirichlet multiplication and addition form a commutative ring. That is:
Suppose f, g, h are arithmetical functions. Then:

a) $f * g$ is also an arithmetical function (closure).

b) $f * I = f$ (identity).

c) $(f * g) * h = f * (g * h)$ (associativity).

d) $f(n)$ is completely multiplicative if and only if it's Dirichlet inverse is $\mu(n)f(n)$.

e) Under addition, the set of arithmetical functions form an abelian group.

Proof.

a) This is clear. $f * g$ is still a function from the naturals to some subset of the complex numbers.

b) $f * I = \sum_{d|n} f\left(\frac{n}{d}\right) I(d)$. If $d \neq 1$ then $I(d) = 0$. The only term left over in this sum is therefore $f(n)I(1) = f(n)$.

c)

$$(f * g) * h = \sum_{d|n} (f * g)(d) h(\frac{n}{d}) =$$

.

$$\sum_{d|n} \left(\sum_{k|d} f(k) g\left(\frac{d}{k}\right) \right) h\left(\frac{n}{d}\right)$$

. This sum is equivalent to

$$\sum_{abc=n} f(a)g(b)g(c). \tag{2}$$

This can be seen by constructing a correspondence between the terms in each sum. Suppose a, b and c are three integers whose product is n. Since ab is a divisor of n the term $\left(\sum_{k|ab} f(k) g(\frac{ab}{k}) \right) h\left(\frac{n}{ab}\right)$ appears in the sum. Since a divides ab the term $f(a)g(\frac{ab}{a})$ appears in inner sum. And so the term $f(a)g(\frac{ab}{a})h(\frac{n}{ab}) = f(a)g(b)h(c)$ appears in the expansion of $(f*g)*h$. The other direction is clear since $k, \frac{d}{k}$, and $\frac{n}{d}$ are integers which multiply to n. The same argument shows that $f * (g * h)$ is also equivalent to (2) so by transitivity: $(f * g) * h = f * (g * h)$.

d) Suppose f is completely multiplicative, then:

$$\sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right) = f(n) \sum_{d|n} \mu(d) = f(n)I(n) = I(n)$$

The final equality is true because $f(1) = 1$. Suppose instead that f has μf as an inverse, then, if $n > 1$:

$$\sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right) = 0$$

In particular, we can take $n = p^a$ for a prime p and we obtain:

$$\mu(1)f(1)f(p)^a + \mu(p)f(p)f(p^{a-1}) = 0$$

This shows that $f(p^a) = f(p)f(p^{a-1})$. We can show by induction that this means $f(p^a) = f(p)^a$ which by Theorem 2.7, part c) is equivalent to f being completely multiplicative.

□

In this ring, the Möbius function has an inverse which is the unit function u as proved in the lemma on the Möbius function. This is the special role it has, as mentioned earlier, and using this fact we can obtain a shorter proof of Theorem 1.5 as follows:

Proof. By Lemma 2.1 part 3, $\phi * u = N$. Taking the Dirichlet product with μ we obtain for the left hand side:

$$(\phi * u) * \mu = \phi * (u * \mu) = \phi * I = \phi$$

. and for the right we obtain $N * \mu = \mu * N$ as required. □

This result, is, in fact more general and used frequently enough to deserve a name.

Theorem 2.7 (Mobius Inversion Formula)**.** For arithmetical functions f and g

$$f(n) = \sum_{d|n} g(d) \text{ if and only if } g(n) = \sum_{d|n} f(d)\mu\left(\tfrac{n}{d}\right).$$

Proof. $f(n) = \sum_{d|n} g(d)$ is equivalent to $f = g * u$. We Dirichlet multiply both sides by μ to obtain: $f * \mu = g * u * \mu = g * I = g$. We can, of course, multiply by u to recover the original equation, which proves the converse. □

We will now generalise this result since it will be useful later when proving the final theorem of this essay, but this first requires a generalisation of of Dirichlet multiplication and a lemma:

Definition 2.5. Suppose F is a real-valued function such that $F(x) = 0$ for $x \in (0, 1)$, and α is an arithmetical function. Then we define:

$$(\alpha \circ (F)(x) = \sum_{1 \leq n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$$

.

Note, $\alpha \circ F$ is another function which shares the property $G(x) = 0$ for $x \in (0, 1)$.

Lemma 2.8. The operation $\circ$ is associative in the following sense: Let α, β be arithmetical functions and F a function with the properties above, then

$$\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F$$

Proof. We have:

$$(\alpha \circ (\beta \circ F))(x) = \sum_{1 \leq n \leq x} \alpha(n) \sum_{1 \leq m \leq \frac{x}{n}} \beta(m) F\left(\frac{x}{mn}\right) = \sum_{1 \leq nm \leq x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right)$$

The sum is the same as:

$$\sum_{k \leq x} \left(\sum_{n|k} \alpha(n) \beta\left(\frac{k}{n}\right) \right) F\left(\frac{x}{k}\right)$$

To see that these are the same, apply the same reasoning as in the proof of associativity for Dirichlet multiplication: both sums go through all products $\alpha(a)\beta(b)F(c)$ where $ab \leq x$ and $abc = x$. The final sum is the same as $((\alpha * \beta) \circ F)(x)$ and we are done. □

If the reader is interested in the algebraic interpretation of this result, note: functions such as F together with arithmetic functions, form a module. This is essentially a vector space over a ring. In this case, arithmetic functions act as scalars. The formal definition is not relevant to the content of this essay, but all the required properties are easily verified.

That said, we now generalise the Möbius inversion formula .

Theorem 2.9 (Generalised Möbius Inversion Formula)**.** If α is completely multiplicative then:

$$G(x) = \sum_{1 \leq n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$$

if and only if

$$F(x) = \sum_{1 \leq n \leq x} \mu(n)\alpha(n) F\left(\frac{x}{n}\right)$$

.

Proof. In the notation we have given so far, $G(x) = \alpha \circ F$. Since α is completely multiplicative, it's Dirichlet inverse is $\alpha^{-1} = \mu(n)\alpha(n)$ and so we can multiply by this inverse:

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} * \alpha) \circ (F) = F$$

. □

We have now developed sufficient results to consider Dirichlet series. Before doing that, we'll note that another possible direction to take arithmetic functions is to consider their growth rates. For example, the final section of this essay considers the growth of a particular function. This is common practice in number theory, especially probabilistic number theory. For a discussion on this, see [6], Chapter 2.

This section closely followed Chapter 2 of [2], with additional comments.

3 Dirichlet Series

Definition 3.1 (Dirichlet Series)**.** A series of the form

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

where $f(n)$ is an arithmetical function is called a Dirichlet series. The $f(n)$ are called Dirichlet coefficients

Note the variable s may be complex, so we use the same definitions for the exponential function and complex exponentiation that are used in MA244.

Definition 3.2. If a is a real number, and b is a complex number then notation a^b is defined to mean $e^{blog(a)}$.

Since a is a real number, there is no need to worry about the complex logarithm. The logarithm here is taken to be the inverse of the exponential function for real values.

The most famous Dirichlet series is the Riemann Zeta function, for which $f(n) = 1$. This is given by $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

We will now prove results from Chapter 11 of [2] about the convergence of Dirichlet series.

Theorem 3.1 (Convergence of Dirichlet Series)**.** Let $s = \sigma + it$. Suppose the Dirichlet series $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ is neither absolutely convergent for every $s \in \mathbb{C}$ or divergent for all s. Then there is some real number σ_a such that $F(s)$ converges absolutely whenever $\sigma > \sigma_a$ and diverges absolutely when $\sigma < \sigma_a$. σ_a is called the abscissa of absolutely convergence.

Proof. Let $s_1 = \sigma_1 + it_1$,$s_2 = \sigma_2 + it_2$ We will show that $|n^{s_1}|$ is less than $|n^{s_2}|$ if $\sigma_1 < \sigma_2$:

$|n^s| = |n^{(\sigma+it)}| = |n^\sigma||n^{it}| = |n^\sigma||e^{log(n)it}|$

Since $|e^{log(n)it}| = 1$ we see that $|n^s| = |n^\sigma|$ and so if $\sigma_1 < \sigma_2$ then

$|n^{s_1}| = |n^{\sigma_1}| < |n^{\sigma_2}| = |n^{s_2}|$. Since $|n^s|$ is independent of the imaginary part of s, the absolute convergence of $F(s)$ depends only on the σ. And so we can call S the set of real numbers σ for which $F(s)$ does not converge absolutely.

This is non-empty by the assumption of the theorem. It is also bounded above: With s_1 and s_2 defined as above, the comparison test shows that if $F(s_1)$ converges absolutely, then so must $F(s_2)$. Therefore if $F(s)$ converges absolutely for s, then s is an upper bound of the set S.

By completeness of the real numbers set S has a least upper bound, call it σ_a.

The aim is now to show σ_a defined in this way satisfies the claimed properties. This is clear because if $\sigma < \sigma_a$ then σ must be in S because if it were not it would be an upper bound by the reasoning above. This would contradict σ_a being an upper bound.

If $\sigma > \sigma_a$ then $\sigma \notin S$ since σ_a is an upper bound, and hence $F(s)$ converges. □

Knowing more about the convergence of these series, we can speak about their products more comfortably. And so we come to a theorem about the form of the products of Dirichlet series:

Theorem 3.2. Suppose $F(s), G(s)$ are given Dirichlet series:

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

and

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}.$$

Then where these series converge absolutely, their product is:

$$F(s)G(s) = \sum_{n=1}^{\infty} (f * g)(n).$$

Proof. Since both series converge absolutely for the s we know the following equality is true:

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{f(n)g(m)}{(mn)^s}.$$

This can be most clearly seen by considering the partial sums.

Furthermore, the series on the right converges absolutely so we can rearrange the terms however we want to give the same answer. If we sum all terms whose denominator is 1^s first, then 2^s and so on we obtain:

$$\sum_{n=1}^{\infty} \frac{h(n)}{n^s}.$$

where $h(n)$ is the sum of terms numerators of those terms whose denominator is n^s. In other words, the sum: $\sum_{dk=n} f(d)g(k)$ which is $(f * g)(n)$. This completes the proof. □

Corollary 3.2.1. Recalling the Dirichlet convulsions we have so far derived we obtain the following relationships:

- $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1/\zeta(s)$.
- $\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$.

Since $u * \mu = I$ we have:
$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{I(n)}{n^s} = 1$ since $I(n) = 1$ for $n = 1$ and 0 otherwise.
Both $\zeta(s)$ and $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ converge for $\sigma > 1$ so this is valid in that halfplane.
The second relationship we obtain from the fact $\phi * u = n$. From this we get:
$\zeta(s) \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} = \zeta(s-1)$
Since $\phi(n) < n$ this series converges for $\sigma > 2$.

4 A Formula For "Probability" k-randomly selected Integers Are Coprime

We are now almost ready to answer the question we asked in Chapter 2. What is the probability that two random numbers are coprime? In fact, we can answer this question for k integers. We define big oh notation.

Definition 4.1. If $g(x) > 0$ for all $x \geq a$ then $f(x) = \mathcal{O}(g(x))$ mean there is a constant M, for which $\left|\frac{f(x)}{g(x)}\right| \leq M$ for all $x \geq a$.
If $f(x) = j(x) + \mathcal{O}(h(x))$ this means the difference $f(x) - j(x) = \mathcal{O}(h(x))$

Theorem 4.1. Suppose we have functions, $f = \mathcal{O}(F)$ and $g = \mathcal{O}(G)$. Then:

i) $f + g = \mathcal{O}(F + G)$

ii) $fg = \mathcal{O}(fG)$

iii) if $f = \mathcal{O}(g)$ then $f + g = \mathcal{O}(g)$

Big oh terms are a way to collect terms based on their growth size, greatly simplifying calculations. Why the above theorems are true, and why we have defined addition and multiplication as we have, can be proved easily. See [4] for short proofs. They are omitted here.

The following proof is an elaboration of a proof given by J.E Nymann in [3]. Here we, as mentioned, are talking about the limit of a probability rather than a probability.

Definition 4.2. $Z_k(t)$ gives the number of coprime $k-$tuples whose entries are less than or equal to t, a real number. In notation: $Z_k(t) = \sum_{\substack{(a_1,a_2,\ldots,a_k)=1 \\ a_i \leq t}} 1$

Lemma 4.2. $\sum_{1 \leq d \leq t} Z_k\left(\frac{t}{d}\right) = [t]^k$.

Where $[x]$ is the greatest integers less than x.

Proof. The proof is almost identical to the proof of Lemma 2.1, part 3.

Here, we use a subscript t to distinguish between tuples and greatest common divisors. That is $(a, b, c)_t$ is a $3-$tuple, while (a, b, c) is the greatest common divisor of a, b and c.
We define $S_d = \{(a_1, a_2, .., a_k)_t : (a_1, a_2, ..., a_k) = d, a_i \leq n \text{ for all } i\}$ and $S = \{(a_1, ..., a_k)_t : a_i \leq n \text{ for all } i\}$. As before, the S_d are a partition of S. We note that $(a_1, ..., a_k) = d$ if and only if $(\frac{a_1}{d}, ..., \frac{a_k}{d}) = 1$. Denoting $a_i^{'} = \frac{a_i}{d}$ we realise the sets $S_d^{'} = \{(a_1^{'}, ..., a_k^{'})_t : (a_1^{'}, ..., a_k^{'}) = 1, a_i^{\prime} \leq \frac{t}{d}\}$ and S_d have the same size due to the mentioned correspondence. The size of $S_d^{'}$ is exactly $Z\left(\frac{t}{d}\right)$ by definition of Z_k.

Therefore:

$$\sum_{1\leq d\leq t} Z_k\left(\frac{t}{d}\right) = \sum_{1\leq d\leq t} |S_d| = [t]^k$$

□

Lemma 4.3. For $t \geq 0$, $Z_k(t) = \frac{t^k}{\zeta(k)} + \mathcal{O}(t^{k-1})$ if $t \geq 3$ and if $t = 2$ then $Z_k(t) = \frac{t^k}{\zeta(k)} + \mathcal{O}(tlog(t))$.

Proof. Using the generalised inversion formula we obtain

$$Z_k(t) = \sum_{1\leq d\leq t} \mu(d)\left[\frac{t}{d}\right]^k$$

$$= \sum_{1\leq d\leq t} \mu(d)\left(\frac{t}{d} + \mathcal{O}(1)\right)^k$$

.

Expanding, we obtain:

$$Z_k(t) = t^k \sum_{1\leq d\leq t} \frac{\mu(d)}{d^k} + t^{k-1} \sum_{1\leq d\leq t} \frac{\mu(d)}{d^{k-1}}\mathcal{O}(1) + ... \sum_{1\leq d\leq t} \mathcal{O}(1).$$

We can, by the properties discussed earlier, rewrite the above as:

$$Z_k(t) = t^k \sum_{1\leq d\leq t} \frac{\mu(d)}{d^k} + t^{k-1}\mathcal{O}\left(\sum_{1\leq d\leq t} \frac{\mu(d)}{d^{k-1}}\right) + ... + \mathcal{O}\left(\sum_{1\leq d\leq t} 1\right)$$

.

Now it only remains to simplify the Big-Os.

We begin with the leftmost term. Ignoring the coefficient of t^k for now, this can be written as:

$$\sum_{1\leq d\leq t} \frac{\mu(d)}{d^k} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^k} - \sum_{d>t}^{\infty} \frac{\mu(d)}{d^k}.$$

We already have shown that

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^k} = \frac{1}{\zeta(k)}$$

.

From this point, it can be seen that to prove the desired result we must show the remaining terms in sum are $\mathcal{O}(t^{k-1})$ when $k \geq 3$ and $\mathcal{O}(tlog(t))$ if $k = 2$.

Firstly,

$$\left|\sum_{d>t}^{\infty} \frac{\mu(d)}{d^k}\right| < \sum_{d>t} \frac{1}{d^k} < \int_{[t]}^{\infty} \frac{1}{x^k} dx = \frac{1}{k-1}\frac{1}{[t]^{k-1}} = \mathcal{O}(1/t^{k-1})$$

Remembering the coefficient of t^k we have so far been ignoring, we see that the first term of this sum is $\frac{t^k}{\zeta(k)} + \mathcal{O}(t)$.

If we ignore the coefficient of t^i, the remaining terms are each of the form:

$$\sum_{1\leq d\leq t} \frac{\mu(d)}{d^i}, i \geq 1$$

When $i > 1$, each of these is $\mathcal{O}(1)$ since they are partial sums of convergent series. However, when $i = 1$ we have:

$$\left|\sum_{1\leq d\leq t} \frac{\mu(d)}{d}\right| < \sum_{1\leq d\leq t} \frac{1}{d} = \mathcal{O}(log(t))$$

Finally, $\mathcal{O}\left(\sum_{1\leq d\leq t} 1\right) = \mathcal{O}(t)$.

Combining these results, we can write:

$$Z_k(t) = \frac{t^k}{\zeta(k)} + \mathcal{O}(t) + \mathcal{O}(t^{k-1}) + \mathcal{O}(t^{k-2}) + ...\mathcal{O}(tlog(t)) + \mathcal{O}(t)$$

If $k = 2$ the dominating term among the $\mathcal{O}$'s becomes $\mathcal{O}(tlog(t))$, otherwise it is $\mathcal{O}(t^{k-1})$. This proves the theorem.

□

The result follows easily from this.

Theorem 4.4. The limit as n goes to infinity of the probability that k coprime numbers picked at random (uniformly) from the set $\{1, 2, ...n\}$ is $\frac{1}{\zeta(k)}$

Proof. The probability of obtaining k coprime elements from the set $\{1, 2, ..., n\}$ is obtained by the ratio of number of possible coprime $k-$tuples to the number of possible $k-$tuples. The fomer is $Z_k(n)$ and the latter is n^k. Following from Lemma 3.5, we have: if $k > 2$:

$$\frac{Z_k(n)}{n^k} = \frac{1}{\zeta(k)} + \mathcal{O}\left(\frac{1}{n}\right)$$

if $k = 2$:

$$\frac{Z_2(n)}{n^2} = \frac{1}{\zeta(2)} + \mathcal{O}\left(\frac{log(n)}{n}\right)$$

In either case, the limit as n goes to infinity of $\frac{Z_k(n)}{n^k}$ is the desired result.

□

In lower dimensions ($k = 2, 3$) one can interpret this as a result about points visible from the origin in a lattice. That is, as in the diagram[1], a point is visible from the origin only if it's coordinates are coprime (red). If they are not, there is another point in the way, as we can see with the line drawn.

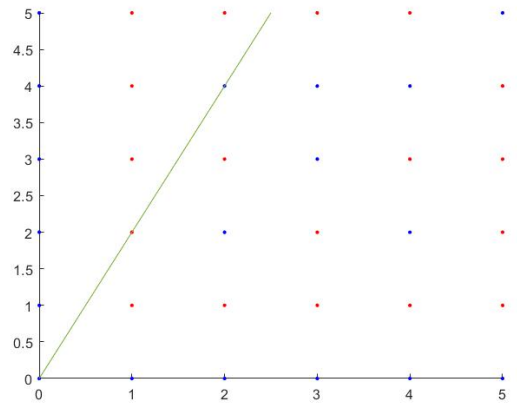

Figure 1: An Integer Latice

5 Appendix

5.1 Notation and Conventions

- The natural numbers, $\mathbb{N}$ will be the set $\{1, 2, 3, ...\}$.
- Throughout this essay, m and n will always be positive natural numbers.
- p will always denote a prime number.
- We will often denote what set we are summing over by a condition below the sigma sign. For example, $\sum_{d|n} f(d)$ means we are summing the values $f(d)$ on each divisor of a given number n.
- (m, n) will denote the greatest common divisor of m and n.

5.2 Results about the Euler Phi and Möbius Functions

Proof of Lemma 2.1.

1. We note that $\phi(n)$ gives the size of the unit group of the ring $\mathbb{Z}/n\mathbb{Z}$. In Algebra 2 it was proved that $\mathbb{Z}/mn\mathbb{Z}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. The theorem follows.

2. Let $f(n)$ count the numbers less than or equal to p^a not coprime to p^a. But these are just every multiple of p less than or equal to p^a. That is kp for $k \in \{1, 2, ..., p^{a-1}\}$. This set clearly contains p^{a-1} elements, so $f(n) = p^{a-1}$ Since a number less than p^a is either coprime to p^a or not $\phi(n) + f(n) = p^a$ from which the desired result follows.

3. Let $S_d = \{k : (k, n) = d, 1 \leq k \leq n\}$. Every element in $S = \{1, 2, ..., n\}$ is in one of the S_d. This is because for $k \in S$ there is some divisor of n, call it a, for which $(k, n) = a$. Furthermore the S_d are disjoint since any integer has exactly one greatest common divisor with n. Therefore the S_d partition S, and $\sum_{d|n} |S_d| = n$. Let's now consider the size of S_d.

We note that $(k, n) = d$ if and only if $(\frac{k}{d}, \frac{n}{d}) = 1$. For clarity, let $q = \frac{k}{d}$. The number of q for which $(q, \frac{n}{d}) = 1$ is $\phi\left(\frac{n}{d}\right)$. And so the size of S_d is $\phi(\frac{n}{d})$. The sum becomes:

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = n$$

But as d goes through the divisors of n so does $\frac{n}{d}$ (since if $d|n$ then there is an integer m such that $n = md$. So $m = \frac{n}{d}$. This proves the theorem.

□

Proof of Theorem 2.2. By the fundamental theorem of arithmetic any integer n can be expressed as a product of prime powers. That is, we can write

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

Inserting this expression into $\phi(n)$ and noting that powers of distinct primes are coprime (allowing us to apply part 1 of Theorem 2.1) we find:

$$\phi(n) = \phi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} \phi\left(p_i^{\alpha_i}\right)$$

By part 2 of Theorem 2.1

$$\phi\left(p^{\alpha_i}\right) = (p^{\alpha_i} - p^{\alpha_i - 1}) = p^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$$

and so

$$\prod_{i=1}^{k} \phi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{k} p^{\alpha_i}\left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

Since $\prod_{i=1}^{k} p_i^{\alpha_i}$ is the prime product form of n and $\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$ goes through the primes dividing n we obtain the required expression.

□

Proof of Theorem 2.3. 1. There are two cases two consider. The first is when one of m or n has a square factor. If one of them does then so does mn and so both $\mu(n)\mu(m)$ and $\mu(mn)$ are 0.

In the second case, neither has a square factor. Suppose n has k prime factors, and m has r prime factors. Since m and n are coprime, all the prime factors between m and n are distinct, and hence so are all those of mn. Thus we obtain:

$$\mu(n)\mu(m) = (-1)^k(-1)^r = (-1)^{r+k} = \mu(mn)$$

2. If n is equal to 1, then it is clear that $\mu(1) = 1$. Suppose $n \geq 1$ and $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ is the prime factor decomposition of n. Consider the non-zero terms of:

$$\sum_{d|n} \mu(d)$$

These are exactly the divisors of n which do not contain square factors. These can be obtained by taking every possible product of distinct primes. Hence the above sum is equal to:

$$\mu(1) + \sum_{p} \mu(p) + \sum_{p_i,p_j} \mu(p_ip_j) + ... + \mu(p_1p_2....p_k)$$

Where the sums are taken over combinations of distinct prime factors dividing n. Of course, μ depends only on how many distinct prime factors, not their amount so we can rewrite as:

$$1 + \sum_{p|n}(-1)^1 + \sum_{p_i,p_j}(-1)^2 + ... + (-1)^k$$

We only need to count the number of combinations of r-tuples of primes dividing n to determine the coefficient of $(-1)^r$ in the above sum. This is $\binom{r}{k}$ and (4) becomes: $1 + \binom{1}{p}(-1)^1 + ...\binom{p}{r}(-1)^r + ...(-1)^k$ which by the binomial formula is exactly $(1-1)^k = 0$

□

Proof of Theorem 2.5.

a) If f is not identically 0 then we have $f(n) \neq 0$ for some n. Since f is multiplicative and $(n, 1) = 1$, we have $f(n) = f(n)f(1)$ and dividing through by the $f(n)$ gives $f(1) = 1$.

b) Assuming f is multiplicative: every $p_i^{a_i}$ is coprime to every $p_j^{a_j}$ where $i \neq j$ and so we can use the multiplicative property repeatedly.

If we instead assume given that the identity holds, then let m and n be coprime integers. Then if $n = p_1^{a_1}...p_r^{a_r}$ and $m = q_1^{b_1}...q_k^{b_k}$ are the prime factor decompositions of n and m we see that:

$$f(mn) = f(p_1^{a_1}...p_r^{a_r})f(q_1^{a_1}...q_k^{a_k}) = f(p_1^{a_1})f(p_2^{a_2})...f(q_1^{b_1})...f(q_k^{b_k}) = f(m)f(n)$$

c) Given f is completely multiplicative, apply this property repeatedly to obtain: $f(p^a) = f(p)f(p^{a-1}) = ... = f(p)^a$.

If we are given $f(p^a) = f(p)^a$ for every prime p and integer $a \geq 1$ then argue the same as in the proof of b).

□

6 Bibliography

References

[1] Graph made in matlab.

[2] T.M. Apostol. *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics. Springer New York, 1998.

[3] J.E Nymann. On the probability that k positive integers are relatively prime. *Journal of Number Theory*, 4(5):469 – 473, 1972.

[4] Marius Overholt. *A Course in Analytic Number Theory (Graduate Studies in Mathematics).* American Mathematical Society, 2014.

[5] Aaron Schlafly and Stan Wagon. Carmichael's conjecture on the euler function is valid below 10ˆ{10,000, 000}. *Mathematics of Computation*, 63(207):415, jul 1994.

[6] Jurgen Spilker Wolfgang Schwarz. *Arithmetical Functions.* Cambridge University Press, 2006.