Introduction to Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

1 Arithmetical Functions

Subsection 1

The Function $[x]$

The Integral and Fractional Parts of a Real Number

- For any real x, denote by $[x]$ the largest integer $\leq x$, i.e., the unique integer such that $x - 1 < [x] \leq x$.
- $[x]$ is called the **integral part** of x.
- $\{x\} = x - [x]$ is called the **fractional part** of x.
- It satisfies $0 \leq \{x\} < 1$.

Properties of the Integral and Fractional Parts

Proposition

Let x, y be real numbers.

- $[x+y] \geq [x]+[y]$;
- for any positive integer n, $[x+n]=[x]+n$;
- $[\frac{x}{n}] = \left[\frac{[x]}{n}\right]$.

- We have $\{x+y\} = \begin{cases} \{x\}+\{y\}, & \text{if } \{x\}+\{y\}<1 \\ \{x\}+\{y\}-1, & \text{if } \{x\}+\{y\}\geq 1 \end{cases}$

  Therefore, $\{x+y\} \leq \{x\}+\{y\}$.

  So $[x+y] = x+y-\{x+y\} = [x]+\{x\}+[y]+\{y\}-\{x+y\} \geq [x]+[y]$.
- $[x+n] = x+n-\{x+n\} = x+n-\{x\} = [x]+n$.
- Suppose $\frac{[x]}{n} = q+\frac{r}{n}$ with $0 \leq r < n$.

  Then $[\frac{x}{n}] = \left[\frac{[x]+\{x\}}{n}\right] = [q+\frac{r}{n}+\frac{\{x\}}{n}] = [q] = \left[\frac{[x]}{n}\right]$.

Max Power of a Prime Dividing a Factorial

Proposition

Let n be a positive integer and p a prime. Suppose $\ell = \max\{k : p^k \mid n!\}$. Then,

$$\ell = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right].$$

- Among the numbers $1, 2, \ldots, n$, there are:
  - $[\frac{n}{p}]$ that are divisible by p;
  - $[\frac{n}{p^2}]$ that are divisible by p^2;

    $\vdots$

  So we get

$$\ell = \sum_{m=1}^{n} \sum_{\substack{j=1 \\ p^j \mid m}}^{\infty} 1 = \sum_{j=1}^{\infty} \sum_{\substack{m=1 \\ p^j \mid m}}^{n} 1 = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right].$$

A Bound on the Max Power

Corollary

Let n be a positive integer and p a prime. Suppose $\ell = \max\{k : p^k \mid n!\}$. Then,

$$\ell \leq \left[\frac{n}{p-1}\right].$$

- Using the preceding proposition, we get

$$\begin{aligned} \ell &= [\tfrac{n}{p}] + [\tfrac{n}{p^2}] + [\tfrac{n}{p^3}] + \cdots \\ &\leq \tfrac{n}{p} + \tfrac{n}{p^2} + \tfrac{n}{p^3} + \cdots \\ &= \tfrac{n}{p}(1 + \tfrac{1}{p} + \tfrac{1}{p^2} + \cdots) \\ &= \tfrac{\frac{n}{p}}{1-\frac{1}{p}} = \tfrac{n}{p-1}. \end{aligned}$$

The result follows, since ℓ is an integer.

Binomial and Multinomial Coefficients

Corollary

Let m, n be positive integers, with $n \le m$. The binomial coefficient

$$\binom{m}{n} = \frac{m!}{n!(m-n)!}$$

is an integer.

- For every prime p:
  - The max power of p dividing $m!$ is $\sum_{j=1}^{\infty} \left[\frac{m}{p^j}\right]$;
  - The max power of p dividing $n!(m-n)!$ is $\sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right] + \sum_{j=1}^{\infty} \left[\frac{m-n}{p^j}\right]$.

  The result follows by noting that $[\frac{m}{p^j}] \ge [\frac{n}{p^j}] + [\frac{m-n}{p^j}]$.
- More generally, if $n_1, \ldots, n_k$ are positive integers such that $n_1 + \cdots + n_k = m$, then the expression $\frac{m!}{n_1! \cdots n_k!}$ is an integer.

Subsection 2

Multiplicative Functions

Multiplicative Functions

- A real function f defined on the positive integers is said to be **multiplicative** if

$$f(m)f(n) = f(mn), \text{ for all } m,n \text{ with } (m,n) = 1.$$

- If f is multiplicative and does not vanish identically then $f(1) = 1$.

  There exists n, such that $f(n) \neq 0$.

  Then, $f(n) = f(n \cdot 1) = f(n)f(1)$. It follows that $f(1) = 1$.
- If f is multiplicative and $n = p_1^{j_1} \cdots p_k^{j_k}$ in standard form then

$$f(n) = f(p_1^{j_1}) \cdots f(p_k^{j_k}).$$

- Thus, to evaluate f, it suffices to calculate its values on the prime powers.

A Further Property of Multiplicative Functions

Proposition

If f is multiplicative and if

$$g(n) = \sum_{d|n} f(d),$$

where the sum is over all divisors d of n, then g is a multiplicative function.

- Suppose $(m,n)=1$.

  Then we have

$$\begin{array}{rcl} g(mn) & = & \sum_{d|mn} f(d) \quad \text{(definition)} \\ & = & \sum_{d|m} \sum_{d'|n} f(dd') \quad ((m,n)=1) \\ & = & \sum_{d|m} f(d) \sum_{d'|n} f(d') \quad \text{(sums)} \\ & = & g(m)g(n). \quad \text{(definition)} \end{array}$$

Subsection 3

Euler's (Totient) Function $\varphi(n)$

Euler's (Totient) Function $\varphi(n)$

- By $\varphi(n)$ we mean the number of numbers $1, 2, \ldots, n$ that are relatively prime to n.

  We have, e.g.,

  $$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2.$$

- We will show, in the next chapter, that φ is multiplicative.

Value of φ on Prime Powers

Proposition

For any prime p,

$$\varphi(p^j) = p^j - p^{j-1}.$$

- There are p^j numbers between 1 and p^j.

  Of those, $\frac{p^j}{p} = p^{j-1}$ are divisible by p.

  So we obtain

  $$\varphi(p^j) = p^j - p^{j-1}.$$

A Formula for $\varphi(n)$

Claim: $\varphi(n) = n\prod_{p|n}(1-\frac{1}{p})$.
Let $p_1,\ldots,p_k$ be the distinct prime factors of n. Then it suffices to show that $\varphi(n)$ is given by

$$n - \sum_r \frac{n}{p_r} + \sum_{r>s} \frac{n}{p_r p_s} - \sum_{r>s>t} \frac{n}{p_r p_s p_t} + \cdots$$

But $\frac{n}{p_r}$ is the number of numbers $1,2,\ldots,n$ that are divisible by p_r; $\frac{n}{p_r p_s}$ is the number that are divisible by $p_r p_s$; and so on. Hence, the above expression is

$$\sum_{m=1}^{n}\left(1 - \sum_{\substack{r \\ p_r|m}} 1 + \sum_{\substack{r>s \\ p_r p_s|m}} 1 - \cdots\right) = \sum_{m=1}^{n}\left(1 - \binom{\ell}{1} + \binom{\ell}{2} - \cdots\right),$$

where $\ell = \ell(m)$ is the number of primes $p_1,\ldots,p_k$ that divide m. Now the summand on the right is $(1-1)^{\ell} = 0$ if $\ell > 0$, and it is 1 if $\ell = 0$, whence the required result follows.

An Alternative Combinatorial Proof

- The formula

$$n - \sum_r \frac{n}{p_r} + \sum_{r>s} \frac{n}{p_r p_s} - \sum_{r>s>t} \frac{n}{p_r p_s p_t} + \cdots$$

can be obtained alternatively as an immediate application of the Inclusion-Exclusion Principle.

The respective sums in the required expression for $\phi(n)$ give the number of elements in the set $1, 2, \ldots, n$ that possess precisely $1, 2, 3, \ldots$ of the properties of divisibility by p_j for $1 \leq j \leq k$;

The Principle (or rather the complement of it) gives the analogous expression for the number of elements in an arbitrary set of n objects that possess none of k possible properties.

A Sum Formula for φ

Proposition

$\sum_{d|n}\varphi(d)=n$.

- As mentioned, φ is multiplicative.

  By a preceding proposition, $g(n)=\sum_{d|n}\varphi(d)$ is also multiplicative.

  For p a prime, we get

$$\begin{array}{rcl} g(p^j) & = & \sum_{d|p^j}\varphi(d)=\varphi(1)+\varphi(p)+\varphi(p^2)+\cdots+\varphi(p^j) \\ & = & 1+(p-1)+(p^2-p)+\cdots+(p^j-p^{j-1})=p^j. \end{array}$$

  Therefore, if $n=p_1^{j_1}\cdots p_k^{j_k}$,

$$g(n)=g(p_1^{j_1}\cdots p_k^{j_k})=g(p_1^{j_1})\cdots g(p_k^{j_k})=p_1^{j_1}\cdots p_k^{j_k}=n.$$

Subsection 4

The Möbius Function $\mu(n)$

The Möbius Function $\mu(n)$

- The **Möbius function** is defined, for any positive integer n, as

$$\mu(n)=\begin{cases} 0, & \text{if } n \text{ contains a squared factor} \\ (-1)^k, & \text{if } n=p_1\cdots p_k \text{ as a product of } k \text{ distinct primes} \end{cases}.$$

By convention, $\mu(1)=1$.

Proposition

μ is multiplicative.

- Suppose $(m,n)=1$. Then $m=p_1^{j_1}\cdots p_k^{j_k}$ and $n=q_1^{i_1}\cdots q_\ell^{i_\ell}$, where $p_1,\ldots,p_k,q_1,\ldots,q_\ell$ are distinct primes.
Now we have

$$\begin{aligned} \mu(mn) &= \mu(p_1^{j_1}\cdots p_k^{j_k}q_1^{i_1}\cdots q_\ell^{i_\ell}) \\ &= \begin{cases} 0, & \text{if any of } j_1,\ldots,j_k,i_1,\ldots,i_\ell>1 \\ (-1)^k(-1)^\ell, & \text{if } j_1=\cdots=j_k=i_1=\cdots=i_\ell=1 \end{cases} \\ &= \mu(p_1^{j_1}\cdots p_k^{j_k})\mu(q_1^{i_1}\cdots q_\ell^{i_\ell})=\mu(m)\mu(n). \end{aligned}$$

The Function $\nu(n)$

- Since the Möbius function is multiplicative, the function
$$\nu(n) = \sum_{d|n} \mu(d)$$
is also multiplicative.
- For all prime powers p^j, with $j > 0$, we have $\nu(p^j) = 0$.
Indeed, we have
$$\begin{array}{rcl} \nu(p^j) & = & \sum_{d|p^j} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^j) \\ & = & 1 + (-1) + 0 + \cdots + 0 = 0. \end{array}$$
- Hence we obtain:
$$\nu(n) = \begin{cases} 0, & \text{if } n > 1 \\ 1, & \text{if } n = 1 \end{cases}$$
If $n = p_1^{j_1} \cdots p_k^{j_k}$,
$$\nu(n) = \nu(p_1^{j_1} \cdots p_k^{j_k}) = \nu(p_1^{j_1}) \cdots \nu(p_k^{j_k}) = \begin{cases} 0, & \text{if } n > 1 \\ 1, & \text{if } n = 1 \end{cases}$$

The Möbius Inversion Formula

Theorem (The Möbius Inversion Formula)

Let f be any arithmetical function, i.e., a function defined on the positive integers. Then

$$g(n) = \sum_{d|n} f(d) \quad \text{iff} \quad f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}).$$

($\Rightarrow$) We have

$$\begin{array}{rcl}\sum_{d|n} \mu(d) g(\frac{n}{d}) & = & \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) \\ & = & \sum_{d'|n} f(d') \nu(\frac{n}{d'}) = f(n).\end{array}$$

($\Leftarrow$) We also have

$$\begin{array}{rcl}\sum_{d|n} f(d) & = & \sum_{d|n} f(\frac{n}{d}) = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(\frac{n}{dd'}) g(d') \\ & = & \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(\frac{n/d'}{d}) \\ & = & \sum_{d'|n} g(d') \nu(\frac{n}{d'}) = g(n).\end{array}$$

Euler and Möbius Functions

Theorem

The Euler and Möbius functions are related by the equation

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

- Using the expression $\varphi(n) = n\prod_{p|n}(1-\frac{1}{p})$, we get

$$\begin{aligned}\varphi(n) &= n\left(1-\sum_{p_i|n}\frac{1}{p_i}+\sum_{p_i,p_j|n}\frac{1}{p_ip_j}-\cdots\right)\\ &= n\left(1+\sum_{p_i|n}\frac{\mu(p_i)}{p_i}+\sum_{p_i,p_j|n}\frac{\mu(p_ip_j)}{p_ip_j}+\cdots\right) = n\sum_{d|n}\frac{\mu(d)}{d}.\end{aligned}$$

- An alternative is to use the formula $n = \sum_{d|n}\varphi(d)$.

  Then, by Möbius Inversion, $\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d} = n\sum_{d|n}\frac{\mu(d)}{d}$.

Möbius Inversion for Functions over the Reals

Theorem

Let f be a real function.

$$\text{If } g(x) = \sum_{n \le x} f(\tfrac{x}{n}), \text{ then } f(x) = \sum_{n \le x} \mu(n) g(\tfrac{x}{n}).$$

- We have

$$\begin{aligned} \sum_{n \le x} \mu(n) g(\tfrac{x}{n}) &= \sum_{n \le x} \sum_{m \le \frac{x}{n}} \mu(n) f(\tfrac{x}{mn}) \\ &= \sum_{\ell \le x} \sum_{m \mid \ell} \mu(\tfrac{\ell}{m}) f(\tfrac{x}{\ell}) \\ &= \sum_{\ell \le x} f(\tfrac{x}{\ell}) \sum_{d \mid \ell} \mu(d) \\ &= \sum_{\ell \le x} f(\tfrac{x}{\ell}) \nu(\ell) = f(x). \end{aligned}$$

Subsection 5

The Functions $\tau(n)$ and $\sigma(n)$

The Functions τ and σ

- For any positive integer n, define:

$$\begin{aligned} \tau(n) &= \text{the number of divisors of } n; \\ \sigma(n) &= \text{the sum of the divisors of } n. \end{aligned}$$

- We have

$$\tau(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d.$$

- Both $\tau(n)$ and $\sigma(n)$ are multiplicative.

  E.g., for $(m,n) = 1$,

$$\tau(m \cdot n) = \sum_{d|mn} 1 = \sum_{(d_1|m, d_2|n)} 1 = \sum_{d_1|m} 1 \cdot \sum_{d_2|n} 1 = \tau(m)\tau(n).$$

Formulas for τ and σ

- For any prime power p^j, we have

$$\begin{aligned}\tau(p^j) &= j+1;\\ \sigma(p^j) &= 1+p+\cdots+p^j = \tfrac{p^{j+1}-1}{p-1}.\end{aligned}$$

- Thus, if p^j is the highest power of p that divides n, then

$$\tau(n) = \prod_{p|n}(j+1), \qquad \sigma(n) = \prod_{p|n}\frac{p^{j+1}-1}{p-1}.$$

Estimates for the Sizes of $\tau(n)$ and $\sigma(n)$

- We have $\tau(n) < cn^{\delta}$, for any $\delta > 0$, where c is a number depending only on δ.

  The function $f(n) = \frac{\tau(n)}{n^{\delta}}$ is multiplicative and satisfies $f(p^j) = \frac{j+1}{p^{j\delta}} < 1$, for all but a finite number of values of p and j. The exceptions are bounded in terms of δ.
- Further, we have

$$\sigma(n) = n \sum_{d|n} \frac{1}{d} \leq n \sum_{d \leq n} \frac{1}{d} < n(1 + \log n).$$

Lower Bound for $\varphi(n)$

- The estimate $\sigma(n) < n(1+\log n)$ implies

$$\varphi(n) > \frac{1}{4}\frac{n}{\log n}, \quad n > 1.$$

In fact the function $f(n) = \frac{\sigma(n)\varphi(n)}{n^2}$ is multiplicative. For any prime power p^j, we have

$$f(p^j) = \sigma(p^j)\frac{\varphi(p^j)}{(p^j)^2} = \frac{p^{j+1}-1}{p-1}\frac{p^j - p^{j-1}}{p^{2j}} = 1 - \frac{1}{p^{j+1}} \geq 1 - \frac{1}{p^2}.$$

But

$$\prod_{p|n}(1-\frac{1}{p^2}) \geq \prod_{m=2}^{\infty}(1-\frac{1}{m^2}) = \frac{1}{2}.$$

So $\sigma(n)\varphi(n) \geq \frac{1}{2}n^2$.
Combining with $\sigma(n) < 2n\log n$, for $n > 2$, we get the bound.

Subsection 6

Average Orders

Average Order of τ

Proposition

For every real x,

$$\sum_{n\leq x}\tau(n)=x\log x+O(x).$$

- We have

$$\sum_{n\leq x}\tau(n)=\sum_{n\leq x}\sum_{d|n}1=\sum_{d\leq x}\sum_{m\leq\frac{x}{d}}1=\sum_{d\leq x}\left[\frac{x}{d}\right].$$

  But $\sum_{d\leq x}\frac{1}{d}=\log x+O(1)$, whence, $\sum_{n\leq x}\tau(n)=x\log x+O(x)$.
- The Proposition implies that

$$\frac{1}{x}\sum_{n\leq x}\tau(n)\overset{x\to\infty}{\sim}\log x.$$

Average Order of σ

Proposition

For every real x,

$$\sum_{n\leq x}\sigma(n)=\frac{1}{12}\pi^2x^2+O(x\log x).$$

- We have

$$\begin{array}{rcl}\sum_{n\leq x}\sigma(n) & = & \sum_{n\leq x}\sum_{d|n}\frac{n}{d}=\sum_{d\leq x}\sum_{m\leq\frac{x}{d}}m \\ & = & \sum_{d\leq x}\frac{1}{2}[\frac{x}{d}]([\frac{x}{d}]+1)=\frac{1}{2}x^2\sum_{d\leq x}\frac{1}{d^2}+O(x\sum_{d\leq x}\frac{1}{d}).\end{array}$$

  But $\sum_{d\leq x}\frac{1}{d^2}=\sum_{d=1}^{\infty}\frac{1}{d^2}+O(\frac{1}{x})=\frac{\pi^2}{6}+O(\frac{1}{x})$, whence, $\sum_{n\leq x}\sigma(n)=\frac{1}{12}\pi^2x^2+O(x\log x)$.
- Since $\sum n\sim\frac{1}{2}x^2$, the "average order" of $\sigma(n)$ is $\frac{1}{6}\pi^2n$.

Average Order of φ

Proposition

For every real x,

$$\sum_{n\leq x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x).$$

- We have

$$\begin{array}{rcl}\sum_{n\leq x}\varphi(n) & = & \sum_{n\leq x}\sum_{d\mid n}\mu(d)\frac{n}{d}=\sum_{d\leq x}\mu(d)\sum_{m\leq\frac{x}{d}}m\\ & = & \sum_{d\leq x}\mu(d)(\frac{1}{2}(\frac{x}{d})^2+O(\frac{x}{d}))\\ & = & \frac{1}{2}x^2\sum_{d\leq x}\frac{\mu(d)}{d^2}+O(x\sum_{d\leq x}\frac{\mu(d)}{d}).\end{array}$$

  But $\sum_{d\leq x}\frac{\mu(d)}{d^2}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O(\frac{1}{x})=\frac{6}{\pi^2}+O(\frac{1}{x})$, whence, $\sum_{n\leq x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x)$.
- Since $\sum n\sim\frac{1}{2}x^2$, the "average order" of $\varphi(n)$ is $\frac{6n}{\pi^2}$.

Probability of Being Relatively Prime

Corollary

The probability that two integers are relatively prime is $\frac{6}{\pi^2}$.

- The experiment consists of drawing an unordered pair of two integers from $1, 2, \ldots, n$ at random.
  The size of the sample space is $n + \binom{n}{2} = n + \frac{n(n-1)}{2} = \frac{n(n+1)}{2}$.
  The samples consisting of relatively prime members are
  $$\varphi(1) + \varphi(2) + \cdots + \varphi(n) = \frac{3}{\pi^2} n^2 + O(n \log n).$$
  Thus, at the limit, the probability of a positive outcome is
  $$\frac{3n^2}{\pi^2} \cdot \frac{2}{n^2} = \frac{6}{\pi^2}.$$

Subsection 7

Perfect Numbers

Perfect Numbers

- A natural number n is said to be **perfect** if

$$\sigma(n) = 2n,$$

i.e., if n is equal to the sum of its divisors other than itself.

Example: 6 and 28 are perfect numbers.

$$\begin{aligned} 6 &= 1+2+3; \\ 28 &= 1+2+4+7+14. \end{aligned}$$

- Whether there exist any odd perfect numbers is a notorious unresolved problem.

Even Perfect Numbers

Theorem

An even number is perfect if and only if it has the form $2^{p-1}(2^p-1)$, where both p and 2^p-1 are primes.

- Suppose, first, that $n = 2^{p-1}(2^p-1)$, where both p and 2^p-1 are primes.

  Note that the list of divisors of n is

$$1, 2, 2^2, \ldots, 2^{p-1}, 2^p-1, 2(2^p-1), \ldots, 2^{p-1}(2^p-1) = n.$$

  Thus, the sum of those divisors $< n$ is:

$$\begin{aligned} &1 + 2 + 2^2 + \cdots + 2^{p-1} + (2^p-1)(1 + 2 + \cdots + 2^{p-2}) \\ &= \tfrac{2^p-1}{2-1} + (2^p-1)\tfrac{2^{p-1}-1}{2-1} \\ &= (2^p-1) + (2^p-1)(2^{p-1}-1) = 2^{p-1}(2^p-1). \end{aligned}$$

Even Perfect Numbers (Converse)

- We now prove the necessity.
  Suppose $\sigma(n)=2n$ and $n=2^k m$, with $k,m>0$ and m odd.
  Then we get
  $$2^{k+1}m=2n=\sigma(n)=\sigma(2^k m)=\sigma(2^k)\sigma(m)=2^{k+1}\sigma(m).$$
  So, for some $\ell>0$, we have $\sigma(m)=2^{k+1}\ell$ and $m=(2^{k+1}-1)\ell$.
  If $\ell>1$, then m would have distinct divisors ℓ,m and 1.
  Thus, $\sigma(m)\geq\ell+m+1$ and $\ell+m=2^{k+1}\ell=\sigma(m)$, a contradiction.
  Thus $\ell=1$ and $\sigma(m)=2^{k+1}=m+1$. So m is a prime.
  Hence, m is a Mersenne prime and, therefore, $k+1$ is a prime p.
  In conclusion, we get $n=2^k m=2^{p-1}(2^p-1)$.

Subsection 8

The Riemann Zeta-Function

The Riemann Zeta Function

- The **Riemann zeta-function** is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s \text{ a complex variable.}$$

- For $s = \sigma + it$, with σ, t real, the series
  - converges absolutely for $\sigma > 1$;
  - converges uniformly for $\sigma > 1 + \delta$, for any $\delta > 0$.

Zeta-Function and Primes: The Euler Product

Theorem (Zeta Function and Euler Product)

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}, \text{ for all } \sigma > 1.$$

- For any positive integer N,

$$\prod_{p \le N} \frac{1}{1 - \frac{1}{p^s}} = \prod_{p \le N} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \sum_m \frac{1}{m^s},$$

where m runs through all the positive integers that are divisible only by primes $\le N$.

Moreover,

$$\left| \sum_m \frac{1}{m^s} - \sum_{n \le N} \frac{1}{n^s} \right| \le \sum_{n > N} \frac{1}{n^\sigma} \xrightarrow{N \to \infty} 0.$$

Möbius Function and Zeta Function

Theorem

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

- We have

$$\begin{aligned}
\zeta(s)\textstyle\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} &= \textstyle\sum_{m=1}^{\infty}\frac{1}{m^s}\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \sum_{m,n=1}^{\infty}\frac{1}{m^s}\frac{\mu(n)}{n^s} \\
&= \textstyle\sum_{m,n=1}^{\infty}\frac{\mu(n)}{(mn)^s} = \sum_{k=1}^{\infty}\sum_{d|k}\frac{\mu(d)}{k^s} \\
&= \textstyle\sum_{k=1}^{\infty}\frac{1}{k^s}\sum_{d|k}\mu(d) = \sum_{k=1}^{\infty}\frac{\nu(k)}{k^s} = 1.
\end{aligned}$$

Euler Function and Zeta Function

Theorem

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

- We have

$$\begin{aligned}
\zeta(s)\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s} &= \sum_{m=1}^{\infty}\frac{1}{m^s}\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s} = \sum_{m,n=1}^{\infty}\frac{1}{m^s}\frac{\varphi(n)}{n^s} \\
&= \sum_{m,n=1}^{\infty}\frac{\varphi(n)}{(mn)^s} = \sum_{k=1}^{\infty}\sum_{d|k}\frac{\varphi(d)}{k^s} \\
&= \sum_{k=1}^{\infty}\frac{1}{k^s}\sum_{d|k}\varphi(d) = \sum_{k=1}^{\infty}\frac{k}{k^s} \\
&= \sum_{k=1}^{\infty}\frac{1}{k^{s-1}} = \zeta(s-1).
\end{aligned}$$

τ and Zeta Function

Theorem

$$(\zeta(s))^2 = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}.$$

- We have

$$\begin{aligned}
(\zeta(s))^2 &= \sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{m,n=1}^{\infty} \frac{1}{m^s} \frac{1}{n^s} \\
&= \sum_{m,n=1}^{\infty} \frac{1}{(mn)^s} = \sum_{k=1}^{\infty} \sum_{d|k} \frac{1}{k^s} \\
&= \sum_{k=1}^{\infty} \frac{1}{k^s} \sum_{d|k} 1 = \sum_{k=1}^{\infty} \frac{\tau(k)}{k^s}.
\end{aligned}$$

σ and Zeta Function

Theorem

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

- We have

$$\begin{aligned}
\zeta(s)\zeta(s-1) &= \sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{n=1}^{\infty} \frac{1}{n^{s-1}} = \sum_{m,n=1}^{\infty} \frac{1}{m^s} \frac{n}{n^s} \\
&= \sum_{m,n=1}^{\infty} \frac{n}{(mn)^s} = \sum_{k=1}^{\infty} \sum_{d|k} \frac{d}{k^s} \\
&= \sum_{k=1}^{\infty} \frac{1}{k^s} \sum_{d|k} d = \sum_{k=1}^{\infty} \frac{\sigma(k)}{k^s}.
\end{aligned}$$