THEORY OF NUMBERS
ARITHMETIC FUNCTIONS

Functions defined on the set of natural numbers.

Definition $f(n)$ is multiplicative $\Leftrightarrow f(uv) = f(u).f(v)$ whenever $(uv) = 1$.

Theorem If $f(n)$ is multiplicative then $F(n) = \sum_{d|n} f(d)$ is also multiplicative.

Proof Let $(uv) = 1$

$$\begin{aligned} F(uv) &= \sum_{d|uv} f(a) \\ &= \sum_{d_1|u} \sum_{d_2|u} f(d_1 d_2) \\ &= \sum_{d_1|u} f(d_1) \sum_{d_2|v} f(d_2) \\ &= F(u)F(v) \end{aligned}$$

For every divisor of $uv \exists$ unique $d_1,\ d_2$ such that $d_1|u\ d_2|v\ d_1 d_2 = 1$.

Definition

$$d(n) = \sum_{d|n} 1$$

$$\sigma(n) = \sum_{d|n} d$$

$d(n)$ and $\sigma(n)$ are both multiplicative. If p is prime the divisors of p^α are $1, p, p^2, \dots, p^\alpha$ therefore

$$\begin{aligned} d(p^\alpha) &= \alpha + 1 \\ \sigma(p^\alpha) &= \frac{p^{\alpha+1} - 1}{p - 1} \end{aligned}$$

Hence if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

$$\begin{aligned} d(n) &= \prod_{i=1}^{k} (\alpha_i + 1) \\ \sigma(n) &= \prod_{i=1}^{k} \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right) \end{aligned}$$

Example For every $\epsilon > 0$, $d(n) = O(n^{\epsilon})$.

Let $D(x) = \sum_{n \leq x} d(n)$ for $x \geq 1$.

Theorem $D(x) = x \log x + (2j-1)x + O\left(x^{\frac{1}{2}}\right)$ for large x, where j is Euler's constant.

Proof We shall first proof that

$$D(x) = 2 \sum_{n \leq x^{\frac{1}{2}}} \left[\frac{x}{n}\right] - \left[x^{\frac{1}{2}}\right]^2 \ \ (x \geq 1)$$

Now $d(n) = \sum_{u,\ u|n} 1 = \sum_{u,v,\ uv=n} 1$. So

$$\begin{aligned}
D(x) &= \sum_{u,\ v\ uv \leq x} 1 \\
&= \sum_{u,\ v\ u \leq x^{\frac{1}{2}} uv \leq x} 1 + \sum_{u,\ v\ u > x^{\frac{1}{2}}\ uv \leq x} 1 \\
&= \sum_{u \leq x^{\frac{1}{2}}} \left[\frac{x}{u}\right] + \sum_{v \leq x^{\frac{1}{2}}} \left\{\left[\frac{x}{v}\right] - \left[x^{\frac{1}{2}}\right]\right\} \\
&= 2 \sum_{u \leq x^{\frac{1}{2}}} \left[\frac{x}{u}\right] - \left[x^{\frac{1}{2}}\right]^2 \\
&= 2 \sum_{n \leq x^{\frac{1}{2}}} \left(\frac{x}{n} + O(1)\right) - \left(x^{\frac{1}{2}} + O(1)\right)^2 \\
&= 2x \sum_{n \leq x^{\frac{1}{2}}} \frac{1}{n} + O(x^{\frac{1}{n}} - x + O(x^{\frac{1}{2}}) \\
&= 2x \left(\log x^{\frac{1}{2}} + j + O\left(\frac{1}{x^{\frac{1}{2}}}\right)\right) - x + O(x^{\frac{1}{2}} \\
&= x \log x + (2j-1)x + O\left(x^{\frac{1}{2}}\right)
\end{aligned}$$

Perfect Numbers A perfect number is one for which $\sigma(n) = 2n$

Theorem (Euclid-Euler) If p is a prime of the from $2^n - 1$ then then number $2^{n-1}p$ is perfect and conversely every even perfect number is of this form.

Proof Suppose

$$\begin{aligned}\sigma(N) &= \sigma(2^{n-1}p) = \sigma(2^{n-1})\sigma(p) \\ &= (2_n - 1)(1+p) = p.2^n = 2N\end{aligned}$$

Suppose N is an even perfect number. Write $N = 2^{n-1}u$ where u is odd, so that $n \geq 2$. Then $2^n u = 2N = \sigma(N) = \sigma(2^{n-1}u) = \sigma(2^{n-1})\sigma(u) = (2^n - 1)\sigma(u)$

i.e. $\sigma(u) = \frac{2^n u}{2^n - 1} = u + \frac{u}{2^n-1}$

$\frac{u}{2^n-1}$ is thus an integer, and it divides u.

$$\begin{aligned}\sigma(u) &= \text{ sum of all divisors of } u \\ &= u + \text{ one divisor of } u\end{aligned}$$

and so this is the only other divisor of u, therefore $u = 2^n - 1$ and u must be prime.

A number is said to be squarefree if it is not divisible by any square > 1.

Möebius function

Möebius inversion formula We define $\mu(1) = 1$ and if $n > 1$

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes} \\ 0 & \text{if } n \text{ is not squarefree} \end{cases}$$

It is easy to see that μ is multiplicative.

Theorem

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & (n = 1) \\ 0 & n > 1 \end{cases}$$

Proof The case $n = 1$ is trivial. If $n > 1$ write $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$

$$\sum_{d|n} \mu(d) = \sum_{d|p_1^{\alpha_1}} \mu(p_1^{\alpha_1} \dots \sum_{d|p_r^{\alpha_r}} \mu(p_r^{\alpha_r})$$

$$\begin{aligned}\sum_{d|p^\alpha} \mu(d) &= 1 + \mu(p) + \mu(p^2) + \dots \mu(p^\alpha) \\ &= 1 - 1 + 0 + \dots + 0 = 0\end{aligned}$$

Alternatively

$$\begin{aligned}\sum_{d|p_1^{\alpha_1}\dots p_r^{\alpha_r}} \mu(d) &= \sum_{d|p_1\dots p_r} \mu(d) \\ &= 1 +^r c_1(-1) +^r c_2(-1)^2 + \dots ^r c_r(-1)^r \\ &= (1-1)^r = 0\end{aligned}$$

Theorem Given $g(n)$ defined on the natural numbers define $f(n) = \sum_{d|n} g(d)$ then $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$

Proof

$$\begin{aligned}\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{t\left|\frac{n}{d}\right.} g(t) \\ &= \sum_{t|n} g(t) \underbrace{\sum_{d\left|\frac{n}{t}\right.} \mu(d)}_{= \begin{matrix} 1 & \text{if } t=n \\ 0 & \text{otherwise}\end{matrix}} \\ &= g(n)\end{aligned}$$

Theorem Suppose $G(x)$ is defined for $x \geq 1$. Define $F(x) = \sum_{n \leq x} G\left(\frac{x}{n}\right)$ $x \geq 1$

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

Proof

$$\begin{aligned}\sum_{n\leq x} \mu(n) F\left(\frac{x}{n}\right) &= \sum_{n\leq x} \mu(n) \sum_{m \leq \frac{x}{n}} G\left(\frac{x}{mn}\right) \\ &= \sum_{u \leq x} G\left(\frac{x}{u}\right) \sum_{m,\ n\ mn=u} \mu(n) \\ &= \sum_{u\leq x} G\left(\frac{x}{u}\right) \sum_{n|u} \mu(n) \\ &= G(x)\end{aligned}$$

Corollary $[x] = \sum_{n\leq x} 1$ therefore $1 = \sum_{n \leq x} \mu(n) \left[\frac{x}{n}\right]$

Euler's function

$$\phi(n) = \sum_{d=1\ (d,n)-1}^{n} 1$$

Theorem **(i)** $\sum_{d|n} \phi(d) = n$

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

(iii) $\phi(n)$ is multiplicative.

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

Proof **(i)** Consider the set $1, 2, \ldots n$ and divide into classes C_d where $r \in C_d \Leftrightarrow (r, n) = d$. C_d is empty unless $D|n$.

Suppose $D|n$ then C_d consists of those r among $1, 2 \ldots n$ for which $(r, n) = d$.

Write $r = dr'$ $n = dn'$ $(r',\ n') = 1$

C_d consists of those r' among $1, 2, \ldots \frac{n}{d}$ such that $\left(r',\ \frac{n}{d}\right) = 1$ therefore C_d contains exactly $\phi\left(\frac{n}{d}\right)$ elements. Therefore

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

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

(iii) $\mu(d)$ is multiplicative and d is multiplicative,

therefore $\frac{\mu(d)}{d}$ is multiplicative,

therefore $\frac{\phi(n)}{n}$ is multiplicative,

n is multiplicative therefore $\phi(n)$ is multiplicative.

(iv) $\phi(1) = 1$

$$\frac{\phi(n)}{n} = \sum_{d|p_1^{\alpha_1}\ldots p_r^{\alpha_r}} \frac{\mu(d)}{d} = \sum_{d|p_1^{\alpha_1}} \frac{\mu(d)}{d} \cdots \sum_{d|p_r^{\alpha_r}} \frac{\mu(d)}{d}$$

$$\sum_{d|p_1^{\alpha_1}} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right)$$

Therefore

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

The Zeta function

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

Theorem
$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

Proof $\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$
$= \left(1 + \frac{1}{2^s} + \frac{1}{(2^2)^s} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{(3^2)^s} + \dots\right)\dots\left(1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + \dots\right)$
$= \sum_{n=1}^{\infty} n^{-s}$

$\zeta(s)$ is a special case of a Dirichlet series $\sum c_n c^{-s}$

We have the following useful result concerning product of Dirichlet series.

$$\sum_{u=1}^{\infty} a_u u^{-s} \sum_{v=1}^{\infty} b_v v^{-s} = \sum_{n=1}^{\infty} c_n c^{-s}$$

where $c_n = \sum_{u,\ v\ uv=n} a_u b_v = \sum_{u|n} a_n b_{\frac{n}{u}}$

In particular

$$\zeta(s) \sum_{u=1}^{\infty} a_u u^{-s} = \sum_{n=1}^{\infty} c'_n n^{-s}$$

where $c'_n = \sum_{u|n} a_u$

Theorem $\mu(n)$ is the coefficient of n^{-s} in $\frac{1}{\zeta(s)}$

$d(n)$ is the coefficient of n^{-s} in $\zeta^2(s)$

$\sigma(n)$ is the coefficient of n^{-s} in $\zeta(s)\zeta(s-1)$

$\phi(n)$ is the coefficient of n^{-s} in $\frac{\zeta(s-1)}{\zeta(s)}$

Proof
$$\zeta(s) \sum_{n=1}^{\infty} \mu(n) n^{-s} = \sum_{n=1}^{\infty} c'_n n^{-s}$$

$$c'_n = \sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

Therefore
$$\zeta(s) \sum_{n=1}^{\infty} \mu(n) u^{-s} = 1$$

These calculations are only formal, and we must verify them in some other way.

$$\begin{aligned}
\frac{1}{\zeta(s)} &= \prod \left(1 - \frac{1}{p^s}\right) \\
&= \left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{5^s}\right)\ldots \\
&= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}
\end{aligned}$$

$\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} c'_n n^{-s},\ c'_n = \sum_{d|n} d = \sigma(n)$

The others are proved in similar ways.

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

Multiply by $\frac{1}{\zeta(s)}$

$$\sum_{n=1}^{\infty} \sum_{d|n} \left(\mu(d)\sigma\left(\frac{n}{d}\right)\right) n^{-s} = \zeta(s-1) = \sum_{n=1}^{\infty} n n^{-s}$$

Therefore

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

This correspond to a Möebius inversion, and whilst the calculations are onlt formal, they are useful to discover relations between the various arithmetic functions.

Example Let $Q(x)$= the number of squarefree numbers not exceeding x.

$$Q(x) = \sum_{n \le x} |\mu(n)|$$

Now

$$\begin{aligned}
\sum n = 1^{\infty} |\mu(n)| n^{-s} &= \left(1 + \frac{1}{2^s}\right)\left(1 + \frac{1}{3^s}\right)\left(1 + \frac{1}{5^s}\right)\ldots \\
&= \prod_p \left(1 + \frac{1}{p^s}\right) \\
&= \frac{\prod \left(1 - \frac{1}{p^s}\right)^{-1}}{\prod \left(1 - \frac{1}{(p^2)^s}\right)^{-1}}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{\zeta(s)}{\zeta(2s)} \\
&= \sum_{a=1}^{\infty} a^{-s} \sum_{b=1}^{\infty} \mu(b) b^{-2s} \\
&= \sum_{n=1}^{\infty} \left(\sum_{a,\ b\ ab^2=n} \mu(b) \right) n^{-s} \\
&= \sum_{n=1}^{\infty} \left(\sum_{b^2|n} \mu(b) \right) n^{-s}
\end{aligned}
$$

Equating coefficients

$|\mu(n)| = \sum_{b\ b^2|n} \mu(b)$.

The calculations are only formal and so we must prove this relation.

Suppose k^2 is the largest square divisor of n, $n = n'k^2$ where n' is squarefree then

$\sum_{b\ b^2|n} \mu(b) = \sum_{b\ b|k} \mu(b) = \begin{matrix} 1 & \text{if } k=1 \\ 0 & \text{otherwise} \end{matrix}$

$k = 1 \Leftrightarrow n$ is squarefree. So

$$
\begin{aligned}
Q(x) &= \sum_{a,\ b\ ab^2 \le x} \mu(b) \\
&= \sum_{b \le x^{\frac{1}{2}}} \mu(b) \sum_{a \le \frac{x}{b^2}} 1 \\
&= \sum_{b \le x^{\frac{1}{2}}} \mu(b) \left[\frac{x}{b^2} \right] \\
&= x \sum_{b \le x^{\frac{1}{2}}} \frac{\mu(b)}{b^2} + O(x^{\frac{1}{2}})
\end{aligned}
$$

Now

$$
\left| \sum_{b > x^{\frac{1}{2}}} \frac{\mu(b)}{b^2} \right| \le \sum_{b \ge x^{\frac{1}{2}}} \frac{1}{b^2} \le \int_{x^{\frac{1}{2}}-1}^{\infty} \frac{dt}{t^2} = O(x^{-\frac{1}{2}}
$$

Therefore $Q(x) = x \sum_{b=1}^{\infty} \frac{\mu(b)}{b^2} + O\left(x^{\frac{1}{2}}\right)$

$\sum \frac{\mu(b)}{b^2} = \frac{1}{\zeta(2)}$

$\zeta(2) = \sum \frac{1}{n^2} = \frac{\pi^2}{6}$

Therefore $Q(x) = \frac{6}{\pi^2}x + O\left(x^{\frac{1}{2}}\right)$

Every large integer can be represented as the sum of two squarefree numbers.

Example on Möebius inversion Pick $a,\ b$ at random. What is the probability that $(a,\ b) = 1$? Define $N(x) = \begin{matrix} 1 \le a \le x \\ 1 \le b \le x \end{matrix}\ (a,\ b) = 1$

Total number of point $= [x]^2$

Probability $= \lim_{x\to\infty} \frac{N(x)}{[x]^2}$

Divide the points $(a,\ b), 1 \le a \le x\ 1 \le b \le x$ into classes C_n where $(a,\ b) \in C_n \Leftrightarrow (a,b) = n$

Each point goes into just one class therefore $[x]^2 = \sum_{n\le x} |c_n|$

Write $a = na'\ b = nb'$ then $1 \le a' \le \frac{x}{n}\ 1 \le b' \le \frac{x}{n}\ (a',b') = 1$

Therefore $|C_n| = N\left(\frac{x}{n}\right)$

Therefore $[x]^2 = \sum_{n\le x} N\left(\frac{x}{n}\right)$

Using the Möebius inversion formula we get

$$\begin{aligned}
N(x) &= \sum_{n\le x} \mu(n) \left[\frac{x}{n}\right]^2 \\
\left[\frac{x}{n}\right]^2 &= \left(\frac{x}{n} + O(1)\right)^2 = \frac{x^2}{n^2} + O\left(\frac{x}{n}\right) + O(1) \\
\text{Therefore } N(x) &= x^2 \sum_{n\le x} \frac{\mu(n)}{n^2} + O(x \sum_{n\le x} \frac{1}{n} \\
&= x^2 \sum_{n\le x} \frac{\mu(n)}{n^2} + O(x \log x) \\
&= x^2 \frac{6}{\pi^2} + O(x \log x) \\
\text{Therefore } \lim_{x\to\infty} \frac{N(x)}{[x]^2} &= \lim_{x\to\infty} \frac{\frac{6}{\pi^2}x^2 + O(x \log x)}{x^2} \\
&= \frac{6}{\pi^2}
\end{aligned}$$