2. Möbius Inversion

Definition 2.1. *Define a function*

$$\pi \colon \mathbb{R} \longrightarrow \mathbb{N}$$

by the rule that $\pi(x)$ is the number of primes up to x.

Theorem 2.2. *If n is a natural number then*

$$\pi(n) > \frac{\log n}{2 \log 2}.$$

In particular there are infinitely many primes.

Proof. Let $k = \pi(n)$.

Consider the square-free integers divisible only by the first k primes numbers, $p_1, p_2, \dots, p_k$. For each prime p_i, we get to choose whether to include p_i or not, so that we can form 2^k square-free natural numbers divisible only by $p_1, p_2, \dots, p_k$.

On the other hand, every natural number up to n is uniquely of the form a perfect square multiplied by a square-free number divisible by only the first k primes. Now there are at at most $\sqrt{n}$ perfect squares at most n, so there are at most $2^k\sqrt{n}$ natural numbers at most n. As there are n natural numbers less than n, we must have

$$\sqrt{n} 2^{\pi(n)} \geq n.$$

Dividing both sides by $\sqrt{n}$, we get

$$2^{\pi(n)} \geq \sqrt{n}.$$

Taking logs of both sides gives

$$\begin{aligned} \pi(n) \log 2 &= \log 2^{\pi(n)} \\ &\geq \log \sqrt{n} \\ &\geq \frac{1}{2} \log n. \end{aligned}$$ □

Note that we could have decided that there were 2^k square-free natural numbers divisible only by the first k primes, by considering how many square-free natural numbers are divisible by exactly l of the first k primes,

$$\binom{k}{l}$$

and summing these to get

$$\binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \dots + \binom{k}{k} = 2^k.$$

Here is a generalisation of this type of argument which is very useful.

Theorem 2.3 (Inclusion-Exclusion)**.** *Let $A_1, A_2, \dots, A_N$ be a collection of N sets. Then*

$$|A_1 \cup A_2 \cup \cdots \cup A_N| = \sum_{i=1}^{N} |A_i| - \sum_{i \neq j} |A_i \cap A_j| + \sum_{\#\{i,j,k\}=3} |A_i \cap A_j \cap A_k|$$

$$- \sum_{\#\{i,j,k,l\}=4} |A_i \cap A_j \cap A_k \cap A_l| + \cdots + (-1)^{N+1} |A_1 \cap A_2 \cap \cdots \cap A_N|.$$

Proof. We just need to check that each element of the union is counted exactly once by the formula on the RHS. Let $x \in A_1 \cup A_2 \cup \cdots \cup A_N$. Suppose that x belongs to $A_{i_1}, A_{i_2}, \dots A_{i_k}$, and to no other sets. By induction on k, we may as well assume that $k = N$, so that x in fact belongs to every A_i.

In this case, note that x contributes one to every possible intersection, since it belongs to every possible intersection of the subsets. So we just need to check that the alternating sum

$$\sum_{i=1}^{N} 1 - \sum_{i \neq j} 1 + \sum_{\#\{i,j,k\}=3} 1 - \sum_{\#\{i,j,k,l\}=3} 1 + \cdots + (-1)^N,$$

is one. The first term is N, since there are N numbers between 1 and N. Put differently there are N subsets with one element. The second term, up to sign, is just the number of subsets with two elements, which is

$$\binom{N}{2}.$$

The third term is the number of subsets with three elements and so on. So we just need to show that

$$N - \binom{N}{2} + \binom{N}{3} - \binom{N}{4} + \cdots + (-1)^{N+1},$$

is equal to one. Now consider expanding

$$0 = (1-1)^N,$$

using the binomial theorem. We would get

$$0 = 1 - \binom{N}{1} + \binom{N}{2} - \binom{N}{3} + \binom{N}{4} + \cdots + (-1)^N.$$

Moving everything but 1 over to the other side, we get

$$N - \binom{N}{2} + \binom{N}{3} - \binom{N}{4} + \cdots + (-1)^{N+1} = 1. \qquad \square$$

Definition 2.4. *Define a function*

$$\mu\colon \mathbb{N} \longrightarrow \mathbb{Z}$$

called the ***Möbius function****, by the rule*

$$\mu(n) = \begin{cases} (-1)^\nu & \text{if } n \text{ is the product of } \nu \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

Thus $\mu(1) = 1 = 1^0$ (the product of zero primes), $\mu(2) = \mu(3) = -1$ and $\mu(4) = 0$.

Lemma 2.5. *The Möbius function μ is multiplicative.*

Proof. Suppose that m and n are two coprime natural numbers.

If m is not square-free then neither is mn and in this case

$$\mu(mn) = \mu(m)\mu(n)$$

as both sides are zero. By symmetry we are also done if n is not square-free.

Therefore we may assume that both m and n are square-free. Suppose that m is the product of μ distinct primes and n is the product of ν distinct primes. In this case mn is the product of $\mu + \nu$ distinct primes and we have

$$\begin{aligned} \mu(m)\mu(n) &= (-1)^\mu(-1)^\nu \\ &= (-1)^{\mu+\nu} \\ &= \mu(mn). \end{aligned}$$ □

Proposition 2.6. *If*

$$M\colon \mathbb{N} \longrightarrow \mathbb{Z},$$

is the function defined by the rule

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

then

$$M(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

Proof. It is clear that $M(1) = \mu(1) = 1$.

Otherwise note that $M(n)$ is multiplicative as $\mu(n)$ is multiplicative. Thus we may assume that n is a power of a prime $n = p^e$. In this case

$$\begin{aligned} M(p^e) &= \sum_{i=0}^{e} \mu(p^i) \\ &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) \\ &= 1 - 1 + 0 + 0 + \cdots + 0 \\ &= 0. \end{aligned}$$

□

Theorem 2.7 (Möbius Inversion). *If $f\colon \mathbb{N} \longrightarrow \mathbb{Z}$ is any function and*

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

then

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} F\left(\frac{n}{d}\right) \mu(d) = \sum_{d_1 d_2 = n} \mu(d_1) F(d_2).$$

Proof. We have

$$\begin{aligned} \sum_{d_1 d_2 = n} \mu(d_1) F(d_2) &= \sum_{d_1 d_2 = n} \mu(d_1) \left(\sum_{d|d_2} f(d) \right) \\ &= \sum_{d_1 d | n} \mu(d_1) f(d) \\ &= \sum_{d|n} f(d) \left(\sum_{d_1 | \frac{n}{d}} \mu(d_1) \right) \\ &= \sum_{d|n} f(d) M\left(\frac{n}{d}\right) \\ &= f(n), \end{aligned}$$

since $M(n/d)$ is zero, unless $n/d = 1$, that is, unless $n = d$, in which case it is one. Thus all but the indicated term of the sum is zero. □

Corollary 2.8.

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

Proof. Note that

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

Note also it was proved in Math 104A that

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

Now apply Möbius inversion. $\square$

Corollary 2.9. *If $f\colon \mathbb{N} \longrightarrow \mathbb{Z}$ is any function and $F\colon \mathbb{N} \longrightarrow \mathbb{Z}$ is defined by the rule*

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

then f is multiplicative if and only if F is multiplicative.

Proof. We have already seen that if f is multiplicative then F is multiplicative.

Now suppose that F is multiplicative. By Möbius inversion we have

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

Let m and n be a coprime natural numbers. We have

$$\begin{aligned} f(m)f(n) &= \left(\sum_{d_1|m} F(d_1)\mu\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} F(d_2)\mu\left(\frac{n}{d_2}\right)\right) \\ &= \sum_{d_1|m, d_2|n} F(d_1)F(d_2)\mu\left(\frac{m}{d_1}\right)\mu\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m, d_2|n} F(d_1d_2)\mu\left(\frac{mn}{d_1d_2}\right) \\ &= \sum_{d|mn} F(d)\mu\left(\frac{mn}{d}\right) \\ &= f(mn). \end{aligned}$$

$\square$