UNIVERSITY OF NEW SOUTH WALES

SCHOOL OF MATHEMATICS AND STATISTICS

Assignment 3

Number Theory

Author:
Edward McDonald

Student Number:
3375335

Question 1

Definition 1. *For an integer $n > 0$, $\omega(n)$ is the number of distinct prime factors of n, and $\Omega(n)$ is number of terms in the prime factorisation of n, that is, if $n = p_1^{k_1} \dots p_m^{k_m}$ where $p_1, p_2, \dots, p_m$ are prime, we have $\omega(n) = m$ and $\Omega(n) = k_1 + k_2 + \dots + k_m$.*

$\tau(n)$ denotes the number of factors of n.

Lemma 1. *For an integer $n > 2$,*

$$2^{\omega(n)} \leq \tau(n) \leq 2^{\Omega(n)} \leq n.$$

Proof. Let $n > 2$ be an integer. Then suppose that n has prime factorisation

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$$

where the numbers $p_1, p_2, \dots, p_m$ are prime and the exponents $k_1, k_2, \dots, k_m$ are positive integers.

Now let $d|n$. Then d has prime factorisation

$$d = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$$

for $0 \leq r_i \leq k_i$ for each $1 \leq i \leq m$. Hence we have $k_i + 1$ possible choices for the exponent of the kth prime factor, and so the total number of choices for d is

$$\prod_{i=1}^{m} (k_i + 1).$$

Hence,

$$\tau(n) = \prod_{i=1}^{m} (k_i + 1).$$

Since by assumption each k_i is positive, we have $k_i \geq 1$, and hence,

$$\tau(n) \geq \prod_{i=1}^{m} (1 + 1) = 2^m = 2^{\omega(n)}.$$

Now note the inequality,

$$x + 1 \leq 2^x$$

valid for $x > 1$ and $p \geq 2$.

So for each i, $k_i + 1 \leq 2^{k_i}$. Hence, we have

$$\tau(n) \leq \prod_{i=1}^{m} 2^{k_i} = 2^{\Omega(n)}.$$

Now since each $p_i \geq 2$, we can bound $2^{\Omega(n)}$ by

$$2^{\Omega(n)} = \prod_{i=1}^{m} 2^{k_i} \leq \prod_{i=1}^{m} p_i^{k_i} = n.$$

Hence, $2^{\omega(n)} \leq \tau(n) \leq 2^{\Omega(n)} \leq n$. □

Lemma 2. $\tau(n) = 2^{\omega(n)}$ *if and only if* n *is square free.*

Proof. Suppose that n is square free. Then n has prime factorisation,

$$n = p_1 p_2 p_3 \cdots p_m$$

for some distinct primes $p_1, p_2, \ldots, p_m$ and $m = \omega(n)$. Hence each factor of n must be of the form

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$

with each exponent $\alpha_k \in \{0, 1\}$ for $1 \leq k \leq m$. Hence there are 2 choices for each exponent, and hence $2^m = 2^{\omega(n)}$ possible factors of n. Then $\tau(n) = 2^{\omega(n)}$.

Now suppose that n is not squarefree, so n has prime factorisation

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}.$$

where each k_i is a positive integer, and at least one of the exponents k_i exceeds 1.

Suppose without loss of generality that $k_1 \geq 2$. Then,

$$\tau(n) = \prod_{i=1}^{n} (k_i + 1) \geq 3 \prod_{i=1}^{n} (k_i + 1) \geq 3 \cdot 2^{m-1} > 2^m.$$

Hence, it is impossible that $\tau(n) = n$ when n is square free. □

Question 2

Definition 2. *For k and n positive integers, define the* Jordan totient function *as*

$$J_k(n) = n^k \prod_{p|n}(1 - p^{-k})$$

where the product is taken over prime factors of n, and $J_k(1) = 1$.

Lemma 3. *J_k is multiplicative.*

Proof. Let n and m be positive integers with $\gcd(n, m) = 1$. Then

$$J_k(nm) = n^k m^k \prod_{p|nm}(1 - p^{-k}).$$

However since n and m share no common prime factors, we may consider

$$J_k(nm) = n^k m^k \prod_{p|n, p|m}(1 - p^{-k}).$$

So we can split up the product,

$$\begin{aligned} J_k(nm) &= \left[n^k \prod_{p|n}(1 - p^{-k})\right]\left[m^k \prod_{p|m}(1 - p^{-k})\right] \\ &= J_k(n)J_k(m). \end{aligned}$$

So J_k is multiplicative. □

Lemma 4. *The function $F(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^k$ is multiplicative.*

Proof. The functions $n \mapsto n^k$ and μ are multiplicative. Since F is the dirichlet convolution of these functions, F is multiplicative. □

Theorem 1.

$$J_k(n) = F(n)$$

where

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

and μ is the Möbius function.

Proof. Since J_k and F are multiplicative, they are determined by their values at prime powers. So let p be prime and let α be a positive integer. Then

$$J_k(p^\alpha) = p^{k\alpha}(1-p^{-k}) = p^{k\alpha} - p^{k(\alpha-1)}$$

and

$$J_k(p^\alpha) = (p^\alpha)^k + \mu(p)(p^{\alpha-1})^k = p^{k\alpha} - p^{k(\alpha-1)}.$$

Hence, $F = J_k$. □

Theorem 2. *If n is a positive integer with prime factorisation $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$, then $J_k^{-1}(n) = (1-p_1^k)(1-p_2^k)\dots(1-p_m^k)$, where the inverse is in the sense of the Dirichlet product.*

Proof. Note that we can write $J_k = \mu * G$, where $G(n) = n^k$. Since G is a completely multiplicative function, $G^{-1} = \mu G$. Hence, since $\mu^{-1} = u$,

$$J_k^{-1} = u * (\mu G).$$

For any any integer $n > 1$,

$$J_k^{-1}(n) = \sum_{d|n} \mu(d)d^k.$$

Note that since J_k^{-1} is a dirichlet convolution of multiplicative functions, J_k^{-1} is multiplicative.

Let p be a prime, and α a non negative integer. Then

$$J_k^{-1}(p^\alpha) = 1 - p^k.$$

Hence, if n has prime factorisation $p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$, then

$$J_k^{-1}(n) = (1-p_1^{k_1})(1-p_2^{k_2})\dots(1-p_m^{k_m}).$$

□

Question 3

Definition 3. *Let $x > 0$. Then we define*

$$M_2(x) = \sum_{n \le x} (\mu(n))^2$$

Lemma 5. *For a positive integer $n \geq 1$,*

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

Proof. Note that

$$(\mu(n))^2 = \begin{cases} 1 \text{ if } n \text{ is square free or } n = 1 \\ 0 \text{ otherwise.} \end{cases}$$

Let

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

Then we need to show that $F(n) = 1$ when n is 1 or square free and 0 otherwise.

Any number n can be expressed as a product of a square and a square free integer. So let $n = a^2q$, where $a \geq 1$ is an integer and q is squarefree. Therefore, $m^2|n$ if and only if $m|a$. Hence,

$$\begin{aligned} F(n) &= F(a^2q) \\ &= \sum_{m|a} \mu(m) \\ &= I(a). \end{aligned}$$

Hence $F(n) = 0$ if $a > 1$ and $F(n) = 1$ if $a = 1$.

Therefore, $F(n) = 0$ when n is not squarefree and 1 otherwise. Hence $F(n) = (\mu(n))^2$). □

Lemma 6.

$$M_2(x) = x \sum_{m \leq x^{\frac{1}{2}}} \frac{\mu(m)}{m^2} - \sum_{m \leq x^{\frac{1}{2}}} \mu(m) \left\{ \frac{x}{m^2} \right\}$$

Proof. Consider the sum

$$M_2(x) = \sum_{n \leq x} (\mu(n))^2.$$

By lemma 5, we can write this as

$$M_2(x) = \sum_{n \leq x} \sum_{m^2|n} \mu(m).$$

The term $\mu(m)$ occurs in this sum when m^2 is a factor of sum integer less than x. There are $\lfloor \frac{x}{m^2} \rfloor$ factors of m^2 less than x, so the term $\mu(m)$ occurs $\lfloor \frac{x}{m^2} \rfloor$ times. Hence, we can express $M_2(x)$ as

$$M_2(x) = \sum_{m \geq 0} \left\lfloor \frac{x}{m^2} \right\rfloor \mu(m)$$

The terms of this sum vanish when $\lfloor \frac{x}{m^2} \rfloor = 0$, which occurs when $m^2 > x$. So $M_2(x)$ can be expressed as

$$M_2(x) = \sum_{m \leq x^{\frac{1}{2}}} \left\lfloor \frac{x}{m^2} \right\rfloor \mu(m).$$

Now write $\lfloor \frac{x}{m^2} \rfloor = \frac{x}{m^2} - \left\{ \frac{x}{m^2} \right\}$ and the result follows. □

Theorem 3. $M_2(x) = \frac{6}{\pi^2} x + \mathcal{O}(x^{\frac{1}{2}})$.

Proof. First note the result,

$$\sum_{n \geq 1} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Hence,

$$\begin{aligned} | \sum_{n \leq x^{1/2}} \frac{\mu(n)}{n^2} | &\leq \frac{1}{\zeta(2)} + \sum_{n \geq x^{1/2}} \frac{1}{n^2} \\ &= \frac{1}{\zeta(2)} + \mathcal{O}(x^{-1/2}). \end{aligned}$$

And also,

$$\begin{aligned} | \sum_{m \leq x^{\frac{1}{2}}} \mu(m) \left\{ \frac{x}{m^2} \right\} | &\leq \sum_{m \leq x^{1/2}} 1 \\ &= \mathcal{O}(x^{\frac{1}{2}}). \end{aligned}$$

So,

$$x \sum_{m \leq x^{\frac{1}{2}}} \frac{\mu(m)}{m^2} - \sum_{m \leq x^{\frac{1}{2}}} \mu(m) \left\{ \frac{x}{m^2} \right\} = x \frac{1}{\zeta(2)} + \mathcal{O}(x^{-\frac{1}{2}}) + \mathcal{O}(x^{\frac{1}{2}}).$$

Therefore,

$$M_2(x) = \frac{6}{\pi^2} x + \mathcal{O}(x^{\frac{1}{2}})$$

as required.

□

Remark 1. *The previous result states that asymptotically, the proposition of square-free numbers in* $[1, x]$ *is* $6/\pi^2$.

Remark 2. *There are* 608 *squarefree numbers in* $1, 2, 3, \ldots, 1000$. *This is in close agreement with the asymptotic formula, since* $6/\pi^2 \approx 0.608$.