Date: Mar 27 Made by Eric

Definition

Definition 1. *An **arithmetic** function $f(n)$ is a function that map all natural numbers to complex numbers*

Definition 2. *An arithmetic function is called **multiplicative** if*

$$f(mn) = f(m)f(n) \tag{1}$$

whenever $gcd(m, n) = 1$

Lemma 1. *A function f is multiplicative if and only if for all $n = p_1^{c_1} \cdots p_k^{c_k}$ we have $f(n) = f(p_1^{c_1}) \cdots f(p_k^{c_k})$*

Proof. From left to right it hold true because prime are co-prime to each other.

From right to left it hold true by simple computation. ■

Definition 3.

$$\tau(n) := \sum_{d|n} 1 \tag{2}$$

$$\sigma(n) := \sum_{d|n} d \tag{3}$$

$$\sigma_k(n) := \sum_{d|n} d^k \tag{4}$$

$$N(n) := n \tag{5}$$

$$u(n) := 1 \tag{6}$$

Lemma 2. *τ and σ are both multiplicative function.*

Proof.

$$\tau(p_1^{c_1} \cdots p_k^{c_k}) = \Pi_{i=1}^k (c_i + 1) = \Pi_{i=1}^k \tau(p_i^{c_i}) \tag{7}$$

$$\sigma(p_1^{c_1} \cdots p_n^{c_n}) = \sum_{d_1=1}^{c_1} \cdots \sum_{d_n=1}^{c_n} \Pi_{i=1}^n p_i^{d_i} = \Pi_{i=1}^n \sum_{d_i=1}^{c_i} p_i^{d_i} = \Pi_{i=1}^n \sigma(p_i^{c_i}) \tag{8}$$

■

Definition 4. *the **identity function** I is defined as*

$$I(n) := \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{if } n > 1 \end{cases} \tag{9}$$

Definition 5. *the **Möubius function** is inductively defined as*

$$I(n) = \sum_{d|n} \mu(d) \tag{10}$$

Lemma 3.

$$\mu(p_1^{c_1} \cdots p_k^{c_k}) = \begin{cases} (-1)^k & c_1 = c_2 = \cdots = c_k \\ 0 & \textit{otherwise} \end{cases} \tag{11}$$

Definition 6. *Let f, g be two arithmetic function. The **Dirichlet product**, or **convolution**, is the arithmetic function $f * g$ given by*

$$f * g(n) := \sum_{de=n} f(d)g(e) \tag{12}$$

Lemma 4.

$$f * g = g * f \tag{13}$$

$$(f * g) * h = f * (g * h) \tag{14}$$

$$f * I = f = I * f \tag{15}$$

Proof.

$$f * g(n) = \sum_{de=n} f(d)g(e) = \sum_{ed=n} g(e)f(d) = g * f(n) \tag{16}$$

$$(f * g) * h(n) = \sum_{de=n} f * g(d)h(e) = \sum_{de=n} \sum_{qr=d} f(q)g(r)h(e) \tag{17}$$

$$= \sum_{qre=n} f(q)g(r)h(e) = \sum_{qm=n} f(q) \sum_{re=m} g(r)h(e) = \sum_{qm=n} f(q)g * h(m) \tag{18}$$

$$= f * (g * h)(n) \tag{19}$$

$$f * I(n) = \sum_{de=n} f(d)I(e) = f(n) = \sum_{ed=n} I(e)f(d) = I * f(n) \tag{20}$$

■

Definition 7. *G denote the set of all arithmetic function f that satisfy $f(1) \neq 0$*

Lemma 5. *$\langle G, * \rangle$ constitute an abelian group*

Proof. Arbitrarily pick f, g from G, we see

$$f * g(1) = f(1)g(1) \neq 0 \tag{21}$$

$$I(1) = 1 \neq 0 \implies I \in G \tag{22}$$

Pick $h(n) = \begin{cases} \frac{1}{f(1)} & n = 1 \\ -\frac{1}{f(1)} \sum_{d|n, d<n} h(d) f(\frac{n}{d}) & n > 1 \end{cases}$ **(This function h is defined by induction)**, and we see

$$f * h(1) = f(1)h(1) = 1 = I(1) \tag{23}$$

$$f*h(n) = \sum_{de=n} h(d)f(e) = h(n)f(1) + \sum_{d|n, d<n} h(d)f(\frac{n}{d}) = h(n)f(1) - h(n)f(1) = 0 \tag{24}$$

So $f^{-1} = h \in G$ ■

Definition 8. *Let f be an arithmetic function ans suppose $f(1) \neq 0$. The **Dirichlet inverse** f^{-1} of f is defined implicitly by $f^{-1} * f = I$*

Theorems

Lemma 6.

$$f(n) = \sum_{d|n} g(d) \implies f = g * u \tag{25}$$

Theorem 7.

$$u * \mu = I \tag{26}$$

Proof.

$$u * \mu(n) = \sum_{de=n} u(d)\mu(e) = \sum_{e|n} \mu(e) = I(n) \tag{27}$$

■

Theorem 8. *Let g, h be multiplicative function*

$$g * h \text{ are multiplicative}$$

Proof.

$$g * h(\Pi_{i=1}^r p_i^{c_i}) = \sum_{de=\Pi_{i=1}^r p_i^{c_i}} g(d)h(e) = \sum_{d_k \leq c_k, \forall k} g(\Pi_{j=1}^r p_j^{d_j})h(\Pi_{j=1}^r p_j^{c_j - d_j}) \tag{28}$$

$$= \sum_{d_k \leq c_k, \forall k} \Pi_{j=1}^r g(p_j^{d_j})h(p_j^{c_j - d_j}) = \Pi_{j=1}^r \sum_{d_i=1}^{c_i} g(p_i^{c_i})h(p_i^{c_i - d_i}) = \Pi_{j=1}^r g * h(p_j^{c_j}) \tag{29}$$

■

Exercises

8.3

Show that for each k, the function $\sigma_k(n) = \sum_{d|n} d^k$ is multiplicative

Proof.

$$\sigma_k(p_1^{c_1} \cdots p_r^{c_r}) = \sum_{d_1=1}^{c_1} \cdots \sum_{d_r=1}^{c_r} \Pi_{i=1}^r p_i^{kd_i} = \Pi_{i=1}^r \sum_{d_i=1}^{c_i} p_i^{kd_i} = \Pi_{i=1}^r \sigma(p_i^{c_i}) \tag{30}$$

■

8.12

Prove that

$$\sum_{d|n} \tau(d)\mu(\frac{n}{d}) = \sum_{d|n} \mu(d)\tau(\frac{n}{d}) = 1 \tag{31}$$

and

$$\sum_{d|n} \sigma(d)\mu(\frac{n}{d}) = \sum_{d|n} \mu(d)\sigma(\frac{n}{d}) = n \tag{32}$$

for all $n \leq 1$. Verify these equations for $n = 12$

Proof. Notice that $\tau(n) = \sum_{d|n} g(d)$ where g is defined by $x \mapsto 1$

Then by Theorem 3, we see

$$\sum_{d|n} \mu(d)\tau(\frac{n}{d}) = g(n) = 1 \tag{33}$$

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

Then by Theorem 3, we see

$$\sum_{d|n} \mu(d)\sigma(\frac{n}{d}) = N(n) = n \tag{34}$$

Let $A = \sum_{d|12} \mu(d)\tau(\frac{12}{d})$ and $B = \sum_{d|12} \mu(d)\sigma(\frac{12}{d})$. Now we verify

$$A = \mu(1)\tau(12)+\mu(2)\tau(6)+\mu(3)\tau(4)+\mu(4)\tau(3)+\mu(6)\tau(2)+\mu(12)\tau(1) \tag{35}$$

$$= \tau(12) - \tau(6) - \tau(4) + 0\tau(3) + \tau(2) + 0\tau(1) \tag{36}$$

$$= 6 - 4 - 3 + 0 + 2 + 0 = 1 \tag{37}$$

$$B = \mu(1)\sigma(12)+\mu(2)\sigma(6)+\mu(3)\sigma(4)+\mu(4)\sigma(3)+\mu(6)\sigma(2)+\mu(12)\sigma(1) \tag{38}$$

$$= \sigma(12) - \sigma(6) - \sigma(4) + 0\sigma(3) + \sigma(2) + 0\sigma(1) \tag{39}$$

$$= 28 - 12 - 7 + 0 + 3 + 0 = 12 \tag{40}$$

■

8.16

Express τ and σ as the convolution of of two simpler arithmetic function

Proof.

$$\tau(n) = \sum_{d|n} 1 = \sum_{de|n} u(d)u(e) = (u * u)(n) \tag{41}$$

$$\sigma(n) = \sum_{d|n} d = \sum_{de|n} N(d)u(e) = (N * u)(n) \tag{42}$$

■

8.18

What arithmetic functions are represented by $\tau * \mu$ and by $\sigma * \mu$

Proof.

$$\tau * \mu = (u * u) * \mu = u * (u * \mu) = u * I = u \tag{43}$$
$$\sigma * \mu = (N * u) * \mu = N \tag{44}$$

■

8.20

Suppose f is multiplicative and $f \neq 0$. Show that

$$f(1) \neq 0 \text{ and } f^{-1} \text{ is multiplicative}$$

Proof. Assume that f^{-1} is not multiplicative, then

$$S := \{(n,m) : gcd(n,m) = 1, f^{-1}(n)f^{-1}(m) \neq f^{-1}(nm)\} \neq \varnothing \tag{45}$$

We pick "a" smallest (n_k, m_k) form S, that is, no $(n,m) \in S$ satisfy $n < n_k$ and $m < m_k$. Notice we use the article "a" because there may be multiple smallest element.

Notice that

$$f(x) = f(x)f(1) \implies f(1) = 1 \tag{46}$$

and that

$$1 = I(1) = f * f^{-1}(1) = f(1)f^{-1}(1) \implies f^{-1}(1) = 1 \tag{47}$$

Keep the fact (n_k, m_k) is the smallest element of S and the equations (45,46) in mind to check the following equivalency.

$$\sum_{a|n_k, b|m_k} f^{-1}(a)f^{-1}(b)f(\frac{n_k}{a})f(\frac{m_k}{b}) = \sum_{d|n_k m_k} f^{-1}(d)f(\frac{n_k m_k}{d}) \tag{48}$$
$$\iff f^{-1}(n_k m_k) = f^{-1}(n_k)f^{-1}(m_k) \tag{49}$$

Notice that once we prove the statement in equation (47) is true, which we prove in the following, we cause a contradiction.

$$\sum_{a|n_k, b|m_k} f^{-1}(a)f^{-1}(b)f(\frac{n_k}{a})f(\frac{m_k}{b}) = \sum_{a|n_k}\sum_{b|m_k} f^{-1}(a)f(\frac{n_k}{a})f^{-1}(b)f(\frac{m_k}{b}) \tag{50}$$
$$= \sum_{a|n_k} f^{-1}(a)f(\frac{n_k}{a}) \sum_{b|m_k} f^{-1}(b)f(\frac{m_k}{b}) = [f^{-1} * f(n_k)][f^{-1} * f(m_k)] \tag{51}$$
$$= I(n_k)I(m_k) = I(n_k m_k) = f^{-1} * f(n_k m_k) = \sum_{d|n_k m_k} f^{-1}(d)f(\frac{n_k m_k}{d}) \text{ CaC} \tag{52}$$

■

8.21

(a)

Define

$$\chi(n) := \begin{cases} 0 & 2|n \\ 1 & n \equiv_4 1 \\ -1 & n \equiv_4 3 \end{cases} \tag{53}$$

Show that

$$\chi \text{ is multiplicative}$$

Proof. We simply try all possible cases ■

(b)

Let $\tau_1(n)$ and $\tau_3(n)$ denote the number of divisors d of n such that $d \equiv_4 1$ or 3 respectively; show that

$$g(n) := \tau_1(n) - \tau_3(n) \text{ is multiplicative}$$

and

find an expression of $g(p^c)$ **(I don't understand WTF this mean so I skip)**

Proof. Observe

$$g(n) = \sum_{d|n} \chi(d) \tag{54}$$

So $g = u * \chi$, where both u and χ are multiplicative, which tell us that g is also multiplicative.

■

8.22

Show that

$$\mu(n) \text{ is the sum of primitive complex } n\text{-th roots of } 1.$$

Proof. We first prove that the two sets below are the same

$$\{\text{complex } n\text{-th roots of } 1\} = \{\text{complex primitive } d\text{-th roots of } 1, d|n\} \tag{55}$$

More precisely, we wish to prove

$$\{\alpha|\alpha^n = 1\} = \bigcup_{d|n} \{\alpha|\alpha^d = 1, \forall 0 < m < d, \alpha^m \neq 1\} \tag{56}$$

It is quite obvious that the right hand side is a subset of the left hand side.

$$\alpha^d = 1 \implies \alpha^n = (\alpha^d)^{\frac{n}{d}} = 1 \tag{57}$$

Now we show that the left hand side is a subset of the right hand side. Arbitrarily pick α from $\{\alpha|\alpha^n = 1\}$, and find the smallest natural number r that satisfy $\alpha^r = 1$. Notice that r must be a divisor of n, otherwise $\alpha^n \neq 1$. Because r is the smallest natural number that satisfy $\alpha^r = 1$, we know $\forall 0 < m < r, \alpha^m \neq 1$. This implies that α belong to the set on the right hand side. (done)

Define $g(d)$ as the sum of primitive complex d-th roots of 1. More precisely

$$g(d) := \sum\{\alpha|\alpha^d = 1, \forall 0 < m < d, \alpha^m \neq 1\} \tag{58}$$

We see

$$g * u(n) = \sum_{d|n} g(d) = \sum \bigcup_{d|n}\{\alpha|\alpha^d = 1, \forall 0 < m < d, \alpha^m \neq 1\} \tag{59}$$

$$= \sum\{\alpha|\alpha^n = 1\} \tag{60}$$

Notice that $\{\alpha|\alpha^n = 1\}$ is the set of solutions to the equation $x^n - 1 = 0$. Factorize $x^n - 1$ into the form $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, we see that $\sum \alpha_i$ is the negate of the coefficient of the $(n-1)$-th term of $x^n - 1$, which is 0 if $n > 1$. In conclusion, $g * u(n) = 0$, if $n > 1$.

It is easy to see that $g * u(1) = 1$, so we conclude

$$g * u(n) = \begin{cases} 0 & n > 1 \\ 1 & n = 1 \end{cases} = I(n) \tag{61}$$

Then we deduce

$$g = g * I = g * u * \mu = I * \mu = \mu \tag{62}$$

■

8.23

Show that if g is multiplicative then both

$$f = \sum_{d^2|n} g(d^2) \text{ and } h = \sum_{d^2|n} g(\frac{n}{d^2}) \text{ are multiplicative} \tag{63}$$

Proof. Let $(n, m) = 1$

$$f(nm) = \sum_{d^2|nm} g(d^2) = \sum_{a^2|n}\sum_{b^2|m} g(a^2b^2) = \sum_{a^2|n}\sum_{b^2|m} g(a^2)g(b^2) \tag{64}$$

$$= \sum_{a^2|n} g(a^2) \sum_{b^2|m} g(b^2) = f(n)f(m) \tag{65}$$

$$h(nm) = \sum_{d^2|nm} g(\frac{nm}{d^2}) = \sum_{a^2|n}\sum_{b^2|m} g(\frac{nm}{a^2b^2}) = \sum_{a^2|n}\sum_{b^2|m} g(\frac{n}{a^2})g(\frac{m}{b^2}) \tag{66}$$

$$= \sum_{a^2|n} g(\frac{n}{a^2}) \sum_{b^2|m} g(\frac{m}{b^2}) = h(n)h(m) \tag{67}$$

■

Chapter 10:

$n = (2^5)(5^2)(13^2)$

$$n = (2^4)i(1-i)^2(2+i)^2(2-i)^2(3+2i)^2(3-2i)^2 \tag{68}$$

$$n = (2^4)i[(2+i)(2-i)(3+2i)^2(1-i)][(2+i)(2-i)(3-2i)^2(1-i)] \tag{69}$$

$$n = 16i[5(13+12i)(1-i)][5(13-12i)(1-i)] = i[20(25-i)][20(1-25i)] \tag{70}$$

$$n = 500^2 + 20^2 \tag{71}$$

Theorem 9. ***(Minkowski Theorem)*** *Given a lattice Λ, if a central-symmetric convex set S have volume larger than $2^nV(F)$ where $V(F)$ is the volume of fundamental region of Λ, then S contain a non-trivial point of Λ*

Theorem 10. *For every prime p that satisfy $p \equiv_4 1$, we have*

$$\exists (a,b) \in \mathbb{Z}^2, p = a^2 + b^2 \tag{72}$$

Proof. Because $p \equiv_4 1$, we know $-1 \in Q_p$. Let $u^2 \equiv_p -1$. Then $(u,1)$ and $(p,0)$ are two linearly independent vectors. Define

$$\Lambda = span\{(u,1),(p,0)\} \tag{73}$$

It is easily seen

$$\forall (x,y) \in \Lambda, p|x^2 + y^2 \tag{74}$$

Let F be the fundamental region of Λ. By

$$B_2(\sqrt{2p}) = 2p\pi > 4p = 2^2V(F) \tag{75}$$

We see there exists $(x,y) \in \Lambda$ such that $x^2 + y^2 < 2p$. Because $p|x^2+y^2$, we know $p = x^2 + y^2$. ■

Chapter 9

Definition 9.

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{u(n)}{n^s} \tag{76}$$

Lemma 11.

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1 \tag{77}$$

Zeta is the Dirichlet series of u

Definition 10.

$$P := Pr((x, y) = 1) \tag{78}$$

Lemma 12.

$$1 = \sum_{n=1}^{\infty} Pr((x, y) = n) = \sum_{n=1}^{\infty} \frac{P}{n^2} = P\zeta(2) \implies P = \frac{1}{\zeta(2)} \tag{79}$$