ALGEBRA NOTE 4

JOHNEW ZHANG

1. Multiplicative Functions

Back to φ function.
Recall, if $gcd(n, m) = 1$, then
$\varphi(mn) = \varphi(n)\varphi(m)$.
Note, $n = p_1^{e_1} \dots p_k^{e_k}$.
Then $\varphi(n) = p^{e_1 - 1}(p-1)\dots$.

Definition 1. *$f : \mathbb{N} \to \mathbb{R}$ is multiplicative if and only if $gcd(m, n) = 1 \implies f(mn) = f(m)f(n)$.*
Then $n = p_1^{e_1} \dots p_k^{e_k}$, then $f(n) = f(p_1^{e_1}) \dots f(p_k^{e_k})$.

Example:
$f(n) = 1, \forall n$.
$f(n) = n, \forall n$.
Less trivial
$f(n) = 2^{\#\text{of distinct prime factors}}$.
Example :
$f(p^e) = 2$.
$f(p_1^{e_1} \dots p_k^{e_k}) = 2^n$.
The number of prime divisor of mn is equal to the number of prime divisor of m + the number of prime factors of n.

Theorem 1. *If g is a multiplicative functions, then $f(n) = \sum_{d|n} g(d)$ is multiplicative.*

Proof. If $gcd(m, n) = 1$, then $f(mn) = \sum_{d|mn} g(d) = \sum_{ab|mn} g(ab) = \sum_{a|n} g(a) \sum_{b|m} g(b) = f(m)f(n)$. □

Example : Let $d(n) =$ the number of divisors of n.
$\sum_{g|6} g = 1 + 2 + 3 + 6 = 12, d(6) = 4$.
$d(n) = \sum_{d|n} 1$.

Lemma 1. *Let $gcd(m, n) = 1$, and $d|mn$. Then d can be written in one and only one way as $d = ab$ with $a|n$ and $b|m$.*

Proof. Let $a = gcd(d, n)$ and $b = gcd(d, m)$.

Then $gcd(a, b) = 1$ and $a|d$, and $b|d$, so $ab|d$.

On the other hand, $d = gcd(d, mn)|gcd(d, n)gcd(d, m) = ab$

So $d|ab$, Thus $d = ab$.

Leave the uniqueness as an exercise. □

⋆ d(n) is multiplicative.

$d(p^e) = e + 1$

So then if $n = p_1^{e_1} \dots p_k^{e_k}$, then $d(n) = (e_1 + 1) \dots (e_k + 1)$.

Example: $d(1000) = d(2^3 5^3) = (3 + 1)(3 + 1) = 16$.

Example: Set $\sigma(n) = \sum_{d|n} d$. So σ is multiplicative.

$\sigma(6) = 12$

$\sigma(4) = 1 + 2 + 4 = 7$.

$\sigma(5) = 1 + 5 = 6$.

If $n = p_1^{e_1} \dots p_k^{e_k}$, what is $\sigma(n)$?

Well

$\sigma(p^e) = 1 + p + \dots + p^e = \frac{p^{e+1}-1}{p-1}$

Then $\sigma(n) = (\frac{p_1^{e_1+1}-1}{p_1})(\frac{p_3^{e_3+1}-1}{p_3})$.

Example:

$n = 1521 = 3^2 13^2$.

Then $\sigma 1521 = (\frac{3^{2+1}-1}{3-1})(\frac{13^{2+1}-1}{13-1}) = 2379$.

2. Perfect Number

Definition 2. *A number is perfect if it is the sum of its positive divisors, Other than itself,* $\sigma(n) = \sum_{d|m} d = 2n$.

Example :

$\sigma(6) = 2 \cdot 6$, 6 is perfect.

$\sigma(28) = 2 \cdot 28$.

How many perfect numbers are there?

I don't know.

Theorem 2. *Let n be an even number. Then n is perfect if and only if $n = 2^{p-1}(2^p - 1)$ for some prime p such that $2^p - 1$ is also prime.*

Proof. Is 2^e perfect

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

What about other even number

Write $n = 2^e m$, where m is odd.

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

If n is perfect, then $\sigma(n) = 2n = (2^{e+1} - 1)\sigma(m)$.

so then $(2^{e+1}-1)\sigma(m) = 2^{e+1}m$.
and thus $2^{e+1}|\sigma(m)$, and $2^{e+1}-1|m$.
So here is a k such that
$m = (2^{e+1}-1)k$.
So $\sigma(m) = 2^{e+1}k$.
so $k|\sigma(m)$.
m and k are both divisors of m.
And $m + k = (2^{e+1}-1)k + k = 2^{e+1}k = \sigma(m)$.
So m has only two divisors and thus m is prime, which implies $k = 1$. Since $= 2^{e+1}-1$ is a prime, $e+1$ is a prime.
Set $p = e+1$ since primes should be called, p. Then $e = p-1$, so $n = 2^{p-1}(2^p-1)$.

To see the other way $\sigma(2^{p-1}(2^p-1)) = \sigma(2^{p-1})\sigma(2^p-1) = 2^p(2^p-1) = 2\cdot 2^{p-1}(2^p-1)$ □

Are there any odd perfect numbers?
Probably no, but we are still not able to show.

Definition 3. *A number of the form 2^n-1 is called a* **Mersenne** *number. And if it is prime, it is called a* **Mersenne** *prime.*

It is not true that if p is prime, 2^p-1 is prime

The answer is not all the time.
Check the properties below.
$2^2-1=3$
$2^3-1=7$
$2^5-1=31$
$2^7-1=127$
$2^{11}-1=7047$ (not prime)
$2^{23}-1=83388607$ (not prime)

Example : If e is odd, p and prime, $\sigma(p^e) = 1 + p + \ldots + p^e =$ even.
but 4 not divide 2n, at most are exponent of p;
in $n = p_1^{e_1}\ldots p_3^{e_3}$ can be odd.

Conjecture: There are infinitely many Mersenne primes.

Identify a multiplicative functions, want to know when
$f(n) = g(n)$.
You need only show that $f(p^k) = g(p^k)$ for all prime powers p^k.

Theorem 3. *For any n, $\sum_{d|n}\varphi d = n$.*

Proof. Since φ is multiplicative, so is $g(n) = \sum_{d|n} \varphi(d)$. Well
$g(p^k) = \sum_{d|p^k} \varphi d = 1 + \varphi(1) + \ldots + \varphi(p^k) = 1 + (p-1) + \ldots + (p^k - p^{k-1}) = p^k$ □

Question : If we have
$f(n) = \sum_{d|n} g(d)$,
can we tell what g is Yes!.
For example : $\sum_{d|n} \varphi d = n$ gives us a formula for φ, and not the simple ugly one.
$\varphi(n) = n - \sum_{d|n, d \neq n} \varphi d$

3. The Simplest Multiplication Function

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

Find a g such that $I(n) = \sum_{d|n} g(d)$.
If p is a prime,
Then $I(p) = 0$.
So we need, $g(p) = -1$, since
$\sum_{d|n} g(d) = g(1) + g(p) = 1 + g(p) = 0$.
So $g(p) = -1$, and $g(1) = 1$.
$\sum_{d|n} g(d) = g(1) + g(p) + g(p^2) = 1 - 1 + 0 = 0$.
So $g(p^2) = 0$.
So g is given on prime power by

$$g(p^e) = \begin{cases} 1 & \text{if } e = 0 \\ 0 & \text{if } e > 1 \\ -1 & \text{if } e = 1 \end{cases}$$

This function has a name and it is called Mobins function, and is denoted as μ.

Definition 4. *μ by*

$$\mu(n) = \begin{cases} (-1)^s & \text{if } n = p \ldots p_s \text{is } n \text{ product of } s \text{ distinct primes} \\ 0 & \text{if } p^2 | n \text{ for some prime} \end{cases}$$

$\mu(1) = 1, \mu(2) = -1, \mu(4) = 0$.

Lemma 2. *μ is multiplicative.*

Proof. Let $m, n \in \mathbb{N}$, with $gcd(m.n) = 1$.
If $p^2 | mn$, then $p^2 | m$ or $p^2 | n$.
So that $\mu(mn) = 0 = \mu(m)\mu(n)$.
Now suppose that m and n are square fine and write $m = p_1 \ldots p_s$ and $m = p_1 \ldots p_t$.

Since $gcd(m, n) = 1$, $p_i \neq p_j$, for any $i \in \{1, 2, \ldots s\}$ and $i \in \{1, 2, \ldots t\}$. Then $\mu(mn) = (-1)^{s+t} = (-1)^t(-1)^s = \mu(m)\mu(n)$. □

Theorem 4. *$I(n) = \sum_{d|n} \mu(d)$.*

Proof. $n = 1$ is pretty obvious. If $n = p^k$, then $I(p^k) = 0$, and $\sum_{d|p^k} \mu(d) = 1 + \mu(p) = 0$.
then

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

□

Theorem 5. *Mobins Inversion*
If $f(n) = \sum_{d|n} g(d)$, then
$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$.

Proof. Assume $f(n) = \sum_{d|n} g(d)$. Then $\sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{d|n}(\sum_{e|\frac{n}{d}} g(e)) = \sum_{ed|n} g(e)\mu(d) = \sum_{e|n} g(e)(\sum_{d|\frac{n}{e}} \mu(d)) = \sum_{e|n} g(e) I(\frac{n}{e}) = g(n)$. □

Ex. We have $n = \sum_{d|n} \varphi(d)$, so $\varphi(n) = \sum_{d|n} \mu(d)(\frac{n}{d})$.
If $n = pq$, $\varphi(pq) = \sum_{d|pq} \mu(d)(\frac{pq}{d}) = pq - q - p + 1 = (p-1)(q-1)$.

Ex: $d(n) = \sum_{d|n} 1$.
so $1 = \sum_{d|n} \mu(d) d(\frac{n}{d})$.

Why is μ interesting?
$\lim_{x \to \infty}(\frac{\pi(x)}{\frac{x}{\log x}}) = 1$.
(Prime Number Theorem)
This is equivalent $\lim_{N \to \infty}(\frac{\sum_{n=1}^{N} \mu(d)}{N}) = 0$.
Conjection : For any $\varepsilon > 0$.
$\lim_{n \to \infty}(\frac{\sum_{n=1}^{N}(\mu(d)}{N^{\varepsilon + \frac{1}{\varepsilon}}}) = 0$.
Riemann Hypothesis.