Class Notes

Connor Gephart

September 30 - October 2 2019

1 September 30

1.1 Combinatorial study of $\phi(n)$

$\phi(p) = p - 1$ if p is prime.

$\phi(p^2) = p(p-1)$ because we get p sets of p-1 numbers

$\phi(p^\alpha) = p^{\alpha-1}(p-1)$
Of the numbers up to p^α, p of them are divisible by p, which is $p^{\alpha-1}$ numbers.
Subtracting these from the total number of numbers, $0top^\alpha - 1 = p^\alpha$.
Thus $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$

1.2 Observation

$$\begin{aligned}
\sum_{k=1}^{n} \phi(p^k) &= \phi(1) + \sum_{k=1}^{n} \phi(p^k) \\
&= \phi(1) + \sum_{k=1}^{n} p^{k-1}(p-1) \\
&= \phi(1) + (p-1)\sum_{k=1}^{n} p^{k-1} \\
&= \phi(1) + (p-1)\sum_{k=0}^{n-1} p^{k} \\
&= \phi(1) + (p-1)\frac{1-p^n}{1-p} \\
&= \phi(1) - (1-p^n) \\
&= \phi(1) - 1 + p^n \\
&= p^n
\end{aligned}$$

Because this is a power of p, we can rewrite this as
$\sum_{d|p^n} \phi(d) = p^n$

1.3 Theorem

For any positive integer n, $\sum_{d|p^n} \phi(d) = n$

- Example: $n = 20$
  $d|20, d = \{1, 2, 4, 5, 10, 20\}$

$$\begin{aligned}\sum_{d|20} \phi(d) &= \phi(1) + \phi(2) + \phi(4) + \phi(5) + \phi(10) + \phi(20) \\ &= 1 + 1 + 2 + 4 + 4 + 8 \\ &= 20\end{aligned}$$

Proof: Let $T_d = \{1 \leq i \leq n | gcd(i, n) = d\}$
Example:
$n = 20, d = 5$

$T_5 = \{5, 15\}, |T_5| = 2$

Because every integer from 1 to n occurs in exactly one set,
$\sum_{d|n} |T_d| = n$

Continuing the example of $n = 20$,

i	$gcd(i, n)$
1	1
2	2
3	1
4	4
5	5
6	2
7	1
8	4
9	1
10	10
11	1
12	4
13	1
14	2
15	5
16	4
17	1
18	2
19	1
20	20

This helps us to create the following sets.

$$\begin{aligned} T_1 &= \{1, 3, 7, 9, 11, 13, 17, 19\} \\ T_2 &= \{2, 6, 14, 18\} \\ T_4 &= \{4, 8, 12, 16\} \\ T_5 &= \{5, 15\} \\ T_10 &= \{10\} \\ T_20 &= \{20\} \end{aligned}$$

The sizes of these sets correspond the various $\phi(d)$ values below.

$$\begin{aligned} |T_1| &= \phi(20) = 8 \\ |T_2| &= \phi(10) = 4 \\ |T_4| &= \phi(5) = 4 \\ |T_5| &= \phi(4) = 2 \\ |T_10| &= \phi(2) = 1 \\ |T_20| &= \phi(1) = 1 \end{aligned}$$

Then the total number of numbers, 1-20 can be calculated from the sizes of these sets. That is, $|T_1| + |T_2| + |T_4| + |T -_5| + |T_10| + |T_20| = 20$

So what is $|T_d|$?

$$\begin{aligned} T_d &= \{ad|1 \leq a \leq \frac{n}{d}, gcd(a, \frac{n}{d} = 1)\} \\ |T_d| &= |\{ad|1 \leq a \leq \frac{n}{d}, gcd(a, \frac{n}{d} = 1)\}| \\ &= \phi(\frac{n}{d}) \end{aligned}$$

Thus,

$$\begin{aligned} n &= \sum_{d|n} |T_d| \\ &= \sum_{d|n} \phi(\frac{n}{d}) && = \sum_{e|n} \phi(e) where e = \frac{n}{d} so e d = n \end{aligned}$$

$n = \sum_{e|n} \phi(e)$ is what we wanted to prove.

1.4 Mobius Function

The Mobius function, $\mu(n)$ is another example of an arithmetic function. The function is defined as follows

$$\begin{cases} 0 & \text{if } p^2|n \text{ for any prime } p \\ 1 & \text{if } n \text{ is divisible by an even number of primes} \\ -1 & \text{if } n \text{ is divisible by an odd number of primes} \end{cases}$$

Another function, $\omega(n) =$ the number of prime factors of n can be used to define the Mobius function in a slightly different way.

$$\begin{cases} 0 & \text{if } p^2|n \\ (-1)^{\omega(n)} & \text{otherwise} \end{cases}$$

Examples:

- $\mu(20) = 0$
- $\mu(30) = (-1)^3 = -1$
- $\mu(1) = 0$
- $\mu(p) = -1$ where p is prime

1.5 Theorem

$\phi(n) = \sum_{d|n} \mu(d)(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})(d) = n(\Pi_{p|n}(1 - \frac{1}{p}))$ where p is prime.

Example: $\phi(20) = 8$

$d|20 = \{1, 2, 4, 5, 10, 20\}$

d	$\mu(d)$	$\frac{n}{d}$
1	1	20
2	-1	10
4	0	5
5	-1	4
10	1	2
20	0	1

$$\begin{aligned} \sum_{d|n} \mu(\frac{n}{d})(d) &= \sum_{d|20} \mu(\frac{20}{d} \\ &= 1(20) - 1(10) + 0(5) - 1(4) + 1(2) + 0(1) \\ &= 20 - 10 - 4 + 2 \\ &= 8 \end{aligned}$$

Using the other formula:

$$\begin{aligned} n(\Pi_{p|n}(1-\frac{1}{p})) &= 20(1-\frac{1}{2})(1-\frac{1}{5}) \\ &= 20(\frac{1}{2})(\frac{4}{5}) \\ &= 20(\frac{4}{10} \\ &= \frac{80}{10} = 8 \end{aligned}$$

2 October 2

2.1 Theorem

$\phi(n) = \sum_{d|n} \mu(d)(\frac{n}{d} = n\Pi_{p|d}(1-\frac{1}{p})$ Proof: Induction on the number of distinctive prime factors of n, $\omega(n)$
Base Case: $n = 1$ holds vacuously because $n = p^\alpha$ has 1 prime factor.

We already know $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1-\frac{1}{p})$

Check that these formulas hold:

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

Thus this formula works. Now for the product formula:

$$p^\alpha\Pi(1-\frac{1}{p} = p^\alpha(1-\frac{1}{p})$$

Both formulas work when n has one prime factor.

Induction Step: Now suppose both formulae hold when n has k prime factors.

Suppose n has $k+1$ prime factors, and suppose p is a prime factor.

$n = p^\alpha \cdot n'$ where $p \nmid n'$

$\omega(n) = k+1, \omega(n') = k$. n' has one fewer prime factors than n. Thus our formulae hold for n'.

Count integers up to n, coprime to n. This is what $\phi(n)$ is.

Take the n integers up to n, and divide them into p^α chunks of n' consecutive integers. This creates p^α subintervals.

Within each subinterval, there are $\phi(n')$ many integers coprime to n'.

In total we have $p^\alpha(\phi(n))$ many integers that are coprime to n' between 1 and n.

But we need to remove the multiples of p to get the number of integers coprime to n instead of n'.

$\frac{1}{p}$ of these numbers are divisible by p.

Thus, $p^\alpha(\frac{1}{p}) = p^{\alpha-1}$

$p^{\alpha-1} \cdot \phi(n')$ of these numbers are divisible by p.

Then $\phi(n) = p^\alpha\phi(n') - p^{\alpha-1}\phi(n')$.

We want to show that this is equal to our formulae.

1. Since $\phi(n') = n'\Pi_{q|n'}(1 - \frac{1}{q}$

$\phi(n) = p^\alpha(n')\Pi_{q|n'}(1 - \dfrac{1}{q}) - p^{\alpha-1}n'\Pi_{q|n}(1 - \dfrac{1}{q})$ At this point we know $p^\alpha(n') = n$ so

$$\begin{aligned}\phi(n) &= n(\Pi_{q|n'}(1 - \frac{1}{q}) - \frac{1}{p}\Pi_{q|n'}(1 - \frac{1}{q}))\\ &= n(\Pi_{q|n'}(1 - \frac{1}{q}) - \Pi_{q|n'}(1 - \frac{1}{q}))\\ &= n\Pi_{q|n}(1 - \frac{1}{p})\end{aligned}$$

2. Want to show $\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$

We know $\phi(n') = \sum_{d|n'} \mu(d) \frac{n'}{d}$

$$\begin{aligned}
\phi(n) &= p^{\alpha}\phi(n') - p^{\alpha-1}\phi(n') \\
&= p^{\alpha} \sum_{d|n'} \mu(d) \frac{n'}{d} - p^{\alpha-1} \sum_{d|n'} \mu(d) \frac{p^{\alpha}(n')}{d} \\
&= \sum_{d|n'} \mu(d) \frac{p^{\alpha}(n')}{d} - \frac{1}{p} \sum_{d|n'} \mu(d) \frac{p^{\alpha}(n')}{d} \\
&= \sum_{d|n'} \mu(d) \frac{n}{d} - \frac{1}{p} \sum_{d|n'} \mu(d) \frac{n}{d} \\
&= \sum_{d|n'} \mu(d) \frac{n}{d} + \sum_{d|n'} \mu(pd) \frac{n}{pd} \\
&= \sum_{d|n, p\nmid d} \mu(d) \frac{n}{d} + \sum_{pd|n, p\nmid d} \mu(pd) \frac{n}{pd}
\end{aligned}$$

Then the following expression evaluates to zero because of the definition of the Mobius function. Each sum over a value of d where d is some divisor of n'.

$\sum_{p^2|n, p\nmid d} \mu(p^2 d) \frac{n}{p^2 d} + \sum_{p^3|n, p\nmid d} \mu(p^3 d) \frac{n}{p^3 d} + ... + \sum_{p^{\alpha}|n, p\nmid d} \mu(p^{\alpha} d) \frac{n}{p^{\alpha} d}$

Then every divisor e of n looks like $e = p^i d$ where $p \nmid d$

$\phi(n) = \sum_{e|n} \mu(e) \frac{n}{e}$ which is what we wanted to prove.

2.2 Corollary

If $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ then $\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})...\phi(p_k^{\alpha_k})$

Proof:

$$\begin{aligned}
\phi(n) &= n\Pi_{p|n}(1 - \frac{1}{p} \\
&= p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k}) \\
&= p_1^{\alpha_1}(1 - \frac{1}{p_1}) p_2^{\alpha_2}(1 - \frac{1}{p_2})... p_k^{\alpha_k}(1 - \frac{1}{p_k}) \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})...\phi(p_k^{\alpha_k})
\end{aligned}$$

by definition of ϕ for prime numbers $\phi(p^{\alpha}) = p^{\alpha}(1 - \frac{1}{p})$

2.3 Theorem

If $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ then $d(n) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1 = d(p_1^{\alpha_1})d(p_2^{\alpha_2})...d(p_k^{\alpha_k})$

Proof: if $n = p^\alpha$, then $d(p^\alpha) = \#\{p^i | p^\alpha\} = \alpha + 1$

Now suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$

Any divisor $d|n$ where $d = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$

For each i, the possible values of β_i are $0 \leq \beta_i \leq \alpha_i$

So there are $(\alpha_i + 1)$ possibilities for the value of β_i

The total number of divisors of n, $d(n) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1 = d(p_1^{\alpha_1})d(p_2^{\alpha_2})...d(p_k^{\alpha_k})$

2.4 Definition

We say that $f(n)$ is multiplicative if $f(nm) = f(n)f(m)$ whenever $gcd(n, m) = 1$

Example:
Both $\phi(n)$ and $d(n)$ are multiplicative.

2.5 Theorem

$\sigma(n) = \sum_{d|n} d$ is multiplicative.
So $\sigma(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})...\sigma(p_k^{\alpha_k}) = (\frac{p^{\alpha+1}-1}{p_1-1}) \cdot ... \cdot (\frac{p_k^{\alpha_k+1}-1}{p_k-1})$

So $\sigma(p^\alpha) = (\frac{p^{\alpha+1}-1}{p-1})$

Proof:
Prime powers:
$\sigma(p^\alpha) = \sum_{i=0}^{\alpha} p^i = \frac{1-p^{\alpha+1}}{1-p} = \frac{p^{\alpha+1}-1}{p-1}$

Now write $n = lk$ where $gcd(l, k) = 1$

If $d|n$, we can write $d = ef$ where $e|l$ and $f|k$

$$\begin{aligned} \sigma(n) &= \sum_{d|n} d \\ &= \sum_{ef|d, e|l, f|k} ef \\ &= (\sum_{e|l} e)(\sum f|kf) \\ &= \sigma(l)\sigma(k) \end{aligned}$$

Therefore σ is a multiplicative function.

Example:
$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$
$\sigma(3)\sigma(4) = (1 + 3)(1 + 2 + 4) = (4)(7) = 28$
$\sigma(12) = \sigma(3)\sigma(4)$

The function $s(n)$ is not multiplicative.

$s(12) = 1 + 2 + 3 + 4 + 6 = 16$
$s(3)s(4) = (1)(1 + 2) = 3$
$16 \neq 3$