MATH 565 Spring 2019 - Class Notes

3/20/19

Scribe: Samantha Rangos

Summary: In this class we discussed ways to find the size of a reduced residue system, $\varphi(n)$. The Möbius Function and the definition of multiplicative functions were introduced.

1 Reduced Residue Systems and Möbius Function

Definition 1. $\varphi(n)$

- *Size of a reduced residue system (mod n)*
- *Count of integers in 1, 2, 3...n with* $gcd(a, n) = 1$
- *If p is prime, then* $\varphi(p) = p - 1$

Case $n = p^k$**,** $\varphi(p^k)$

From the numbers 1, 2, 3... p^k, we have to remove all multiples of p.

How many of these numbers are divisible by p?

p, 2p, 3p, 4p...$p^k = p(p^k - 1)$

The number of integers divisible by p is $\frac{p^k}{p} = p^{k-1}$.
The number of integers that are coprime is $p^k - p^{k-1}$, thus $\varphi(p^k) = p^k - p^{k-1}$.

If k=1, $\varphi(p^1) = p^1 - p^0 = p - 1$.

Observation: $\varphi(p^k) = p^k - p^{k-1}$

$p^k = p^k - p^{k-1} + p^{k-1} - p^{k-2} + p^{k-2} ... + p - 1 + 1$

$= \varphi(p^k) + \varphi(p^{k-1}) + \varphi(p^{k-2}) + ... + \varphi(p) + \varphi(1)$

We could write this as:

$$p^k = \sum_{j=0}^{k} \varphi(p^j) = \sum_{d|p^k} \varphi(d)$$

Theorem 1. *For any integer n,*

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

Proof. Let $T_d(n)$ be the set of numbers from 1, 2, ... n which have $gcd(a, n) = d$.

Note: $T_1(n)$ = reduced residue system

Let $\#T_d(n)$ be the size of this set, then $n = \sum_{d|n} \#T_d(n)$

because every number from 1 to n is in exactly one set $T_d(n)$.

The set $\#T_d(n)$ contains all the numbers which have gcd d with n. This set is contained in the numbers $d, 2d, 3d...(\frac{n}{d})d$.

So, $T_d(n)$ =$\{ad$: with $gcd(ad, n) = d\}$
$gcd(a, \frac{n}{d} = 1 \iff gcd(ad, n) = d$

$\#T_d(n) = \#\{a \in \{1, 2, ...\frac{n}{d}\} : gcd(a, \frac{n}{d} = 1\}$

$=\varphi(\frac{n}{d})$

$n = \sum_{d|n} \#T_d(n) = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{dd^1=n} \varphi(d^1) = \sum_{d|n} \varphi(d)$

□

Ex: n=12

$\sum_{d|n}(\varphi(\frac{n}{d}) = \varphi(\frac{12}{1}) + \varphi(\frac{12}{2}) + \varphi(\frac{12}{3}) + \varphi(\frac{12}{4}) + \varphi(\frac{12}{6}) + \varphi(\frac{12}{12})$

$= \varphi(12) + \varphi(6) + \varphi(4) + \varphi(3) + \varphi(2) + \varphi(1)$

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

Definition 2. *The Möbius Function*

$\mu(n) = \begin{cases} 0, \text{ if } p^2|n \text{ for some } p \text{ or } (-1)^k, \text{ where } n = p_1p_2p_3...p_k \end{cases}$

Ex:

$\mu(3) = -1$

$\mu(5) = -1$

$\mu(6) = 1$

$\mu(12) = 0$

$\mu(50) = 0$

$\mu(250) = 0$

$\mu(16) = 0$

$\mu(30) = -1$

Theorem 2.

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\prod_{p|n}(1 - \frac{1}{p})$$

Proof. Induction on k, the number of distinct prime factors of n.

Base Case: $k = 0 \rightarrow$n=1

$\varphi(1) = \sum_{d|1} \mu(d) \frac{1}{d} = 1$

$= 1 \prod_{p|1} (1 - \frac{1}{p}) = 1$

$k = 1 \rightarrow n = p^\alpha$
$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

$\sum_{d|p^\alpha} \mu(d) \frac{n}{d} =$

$\sum_{i=0}^{\alpha} \mu(p^i) \frac{p^\alpha}{p^i}$

$= \mu(p^0) p^\alpha + \mu(p^1) \frac{p^\alpha}{p} + ... + \mu(p^\alpha)(1)$
$= p^\alpha - p^{\alpha-1}$

$p^\alpha \prod_{q|p^\alpha} (1 - \frac{1}{q}) = p^\alpha (1 - \frac{1}{p}) = p - p^{\alpha-1}$

Now suppose this works for all integers with k distinct prime factors.

Suppose n has $k + 1$ distinct prime factors.

Write $n = p^\alpha n^1$ and $p \nmid n^1$

Note: n^1 has k prime factors.

Compute $\varphi(n) = \varphi(p^\alpha n^1)$

Count integers from 1 to n having no factors in common with n^1 or p^α.

We know that the number of integers between 1 and n^1 with no prime factors in common with n^1 is $\varphi(n^1) = \sum_{d|n^1} \mu(d) \frac{n^1}{d} = n^1 \prod_{q|n^1} (1 - \frac{1}{q})$ by induction.

And the number of integers less than p^α coprime to p^α is $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

If we take a b with $1 \leq b \leq n$ with $gcd(b, n) = 1$, we must have $gcd(b, n^1) = 1$ and $gcd(b, p^\alpha) = 1$ since $n = p^\alpha n^1$.

By the Chinese Remainder Theorem, every such integer arises as a number coprime to n^1 and an integer coprime to p^α.

So the total number is $\varphi(n^1)\varphi(p^\alpha)$. (Basic Combinatorial Principle)

$\varphi(n) = \varphi(n^1)\varphi(p^\alpha) = (\sum_{d|n^1} \mu(d) \frac{n^1}{d})(p^\alpha - p^{\alpha-1}) = p^\alpha \sum_{d|n^1} \mu(d) \frac{n^1}{d} - p^{\alpha-1} \sum_{d|n^1} \mu(d) \frac{n^1}{d}$

$= \sum_{d|n^1} \mu(d) \frac{n}{d} - \frac{1}{p} \sum_{d|n^1} \mu(d) \frac{n}{d}$

$= \sum_{\substack{d|n \\ p\nmid d}} \mu(d) \frac{n}{d} - \frac{1}{p} \sum_{\substack{d|n \\ p\nmid d}} \mu(d) \frac{n}{d}$

$= \sum_{\substack{d|n \\ p\nmid d}} \mu(d) \frac{n}{d} + \sum_{\substack{d|n \\ p\nmid d}} \mu(pd) \frac{n}{pd} = \sum_{\substack{d|n \\ p\nmid d}} \mu(d) \frac{n}{d} + \sum_{\substack{d|n \\ p\nmid d}} \mu(pd) \frac{n}{pd} + \sum_{\substack{d|n \\ p\nmid d}} \mu(p^2 d) \frac{n}{p^2 d} + \sum_{\substack{d|n \\ p\nmid d}} \mu(p^3 d) \frac{n}{p^3 d} +$

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

Every divisor of n looks like $p^1 d$ where $p\nmid$d

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

The proof is complete after repeating the same process for $\prod$.

□

Corollary 1. *If* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$*, then*

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$$

Definition 3. *A function* $f(n)$ *is multiplicative if* $f(nm) = f(n)(m)$ *when* $gcd(m,n) = 1$.

Examples of Multiplicative Functions:

- $\varphi(n)$
- $\mu(n)$
- $d(n) = \sum_{d|n} 1$
- $\sigma(n) = \sum_{d|n} d$