Math 152 Notes

Lucas Garron

October 1, 2009

20091001

Hello!

Today: Chinese Remainder Theorem, Euler Phi Function, Multiplicative Functions.

Remember: $\phi(m) = \#$ of residues mod m prime to p.
$\phi(p) = p - 1$ since $\bar{1}, \bar{2}, ..., \bar{p}$ are the residue notations.
$\bar{a} = \{x \in Z | x \equiv a \bmod m\}$

If $\bar{a} = \bar{b} \Rightarrow (a, m) = (b, m)$
$a + Nm = b$, any common divisor of a, b divides $a + Nm$, so any common divisor of b, m $\Rightarrow$ greatest common divisor $(a, m) = (b, m)$.

$\phi(p) = p - 1$
$\phi(p^k) = p^k - pk - 1 (k > 0)$ (p^k classes, p^{k-1} not prime to p)

Theorem: If $(m, n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n)$
Def. If f is a function s.t. $(m, n) = 1 \Rightarrow f(mn) = f(m)f(n)$, f is called <u>multiplicative</u>. (e.g. ϕ)
First:
Thm: $\sum_{d|n} \phi(d) = n$
(Ex. n=12:
d, $\phi(d)$: 1, 1
2, 1
3, 2
4, 2
6, 2
2, 4
$\sum = 12$)
Proof: Enumerate fractions $\frac{a}{n}$ with $a \leq a \leq n - 1$:
$\frac{0}{12}, \frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}$
$= \frac{0}{1}, \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}$
Number of reduced fracs $= a/n$ having denominator d is $\phi(d)$ because there are $\frac{a'}{d}$ with $(a', d) = 1$ and $0 \leq a' \leq d$.

<u>Chinese Remainder Theorem</u>: Suppose $(m, n) = 1$ and a, b are given. Then $\exists k$ s.t. $k \equiv a \bmod m$

and $k \equiv b \bmod n$ <u>and</u> the residue class of k is uniquely determined.

Consider rings Z_m, Z_n, Z_{mn}.
$\exists$ a map p, $p : Z_{mn} \to Z_m$. sending the res. class of a mod mn to the res. class. of a mod m. This is <u>well-defined</u>: If $a \equiv a'$ mod $mn \Rightarrow a \equiv a'$ mod n so this does not depend on the choice of the representative a.
Similarly, $\exists$ a map q, $q : Z_{mn} \to Z_n$, res. class f a to res. class of a.
Ex. $m = 10, n = 11, a = \bar{3}1$: $p(a) = \bar{1}, q(a) = \bar{9}$

$\psi : Z_{mn} \to Z_m \times Z_n = \{\text{ordered pairs}(x, y) | x \in Z_m, y \in Z_n\}$
$(\psi(x) = (p(x), q(x)))$
Claim: ψ is a bijection.
Pigeonhole principle: If x, y are finite sets of some cardinality, $f : x \to y \Rightarrow f$ is injective $\Leftrightarrow$ surjective $\Leftrightarrow$ bijective.
Sufficient to show ψ is injective: suppose $\psi(\bar{x}) = \psi(\bar{y})$
$p(\bar{x}) = p(\bar{y}) \Rightarrow x \equiv y$ mod m. $q(\bar{x}) = q(\bar{y}) \Rightarrow x \equiv y$ mod n. $m | x - y$ and $n | x - y$, but m, n are coprime, so mn (their LCM) divides $x - y$, $x \equiv y$ mod $mn \Rightarrow \bar{x} = \bar{y}$, proving injectivity.

$m = 10, n = 11, a = 7, b = 8$: $107 \equiv -3$
Using Euclidean Algorithm, based on ddiv. alg., we can effectively express GCD(m, n) as a lin. comb. of m, n.
Given a, want $k \equiv a \bmod m$, $k \equiv b \bmod n$
$I = tm + un$
$tmb + una \equiv una = a \bmod m$
$tmb + una \equiv tmb = b \bmod n$

Theorem: If $GCD(m, n) = 1 \Rightarrow \phi(m, n) = \phi(m)\phi(n)$
Res. classes modmn ay be enumerated using CRT.
Let a run through R. C. $modm$, b run through n.
For each a, b let $k = k(a, b)$ be unique R.C. modmn with $k \equiv a \bmod m$, $k \equiv b(n)$ observe $GCD(k, m) = GCD(a, m)$ and $GCD(k, n) = GCD(k, n)$

Suppose $f : N \to C$ is some fn.
$\displaystyle\sum_{n=1}^{\infty} \frac{f(n)}{n!} = F(s)$ is a Dirichlet series.
Riemann Zeta Function:
$\displaystyle\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^r}$ converges absolutely if $Re(s) > 1$ (Integral test.)
If F is multiplicative, then $F(s)$ has an "Euler product".
$\displaystyle\zeta(s) = \prod_p (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + ...)$ using unique factorization.
$\prod^{-s/2} \Gamma(s/2) = \zeta(s)$
$q\prod_{n=1}^{\infty}(1 - q^{24n})^(-1) = q + 24q^2 + 25q^3 + ... = \sum_{n=1}^{\infty} \tau(n)q^n$
τ is multiplicative: $L(s) = \sum \frac{\tau(n)}{n^2} = \prod_p (1 - \tau(p)p^{-2} + p^{11-2s})^{-1}$
$\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}$ should have an Euler product:

$= \frac{\zeta(s-1)}{\zeta(s)}$

(Check: $\zeta(s)\frac{\sum \phi(n)}{n^s} = \zeta(s-1)$

$LHS = \sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{n=1}^{\infty} \phi(n) \frac{1}{n^s}$

$= \sum_{m,n} \frac{\phi(n)}{(mn^2)} = \sum_{m=1}^{\infty} \frac{\sum_{n|m} \phi(n)}{m^s}$

$= \sum_{m=1}^{\infty} \frac{m}{m^s} = \sum_m \frac{1}{m^{s-1}}$

$\sum_{d|n} \phi(d) = n$, $\sum_{n|m} \phi(n) = M$

$\frac{\zeta(s-1)}{\zeta(s)} = \prod_p (1-p^{1-s})^{-1} / \prod_p (1-p^{-s})^{-1} = \prod_{s=1}^{\infty} \frac{1-p^s}{1-p^{1-s}}$

)

Bad notes; Failed attempt at using CRT:

IGNORE: you can find t, u with $tm + un = 1$. So assuming $\exists k$, take these and multiply by k:
IGNORE: $k \equiv tmk + unk(mn)$
IGNORE: $a \equiv k \equiv unk \bmod m$
IGNORE: $v \bmod n$ with $vun \equiv 1 \bmod m$
IGNORE: $w \bmod n$ with $wtn \equiv 1 \bmod n$
IGNORE: Then $k = va + wb$ should work. $kun = vuna + wunb$.