Number Theoretic Functions

CS201A Project

Deepanshu Bansal   Mukul Chaturvedi

Department of Computer Science
IIT KANPUR

Presentaion, $5^{th} Nov, 2016$

Number Theoretic Functions

We will be talking about the following topics in brief.

- $\tau(n)$,the number of positive divisors of n.
- $\sigma(n)$, the sum of positive divisors of n.
- Multiplicative Functions.
- Mobius inversion formula.
- $\phi(n)$, the number of positive integers not exceeding n that are relatively prime to n.

$\tau(n)$

- $\tau(n)$,the number of positive divisors of n.
- n $= p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ is prime factorization of n > 1, then $\tau(n) = (k_1 + 1)(k_2 + 1)...(k_r + 1)$.
- d $= p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ are divisors of n, where0 $\leq \alpha_i \leq$ k$_i$.
- There are $k_1 + 1$ choices for α_1; $k_2 + 1$ choices for α_2...; $k_r + 1$ choices for α_r; hence there are $(k_1 + 1)(k_2 + 1)...(k_r + 1)$ number of divisors of n.

$\sigma(n)$

- $\sigma(n)$,the sum of positive divisors of n.
- n $= p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ is prime factorization of n ≥ 2, *then* $\tau(n) = (k_1 + 1)(k_2 + 1)...(k_r + 1)$.
- $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \frac{p_2^{k_2+1}-1}{p_2-1} ... \frac{p_r^{k_r+1}-1}{p_r-1}$.
- Consider the product $(1 + p_1^1 + p_1^2 ... p_1^{k_1})(1 + p_2^1 + p_2^2 ... p_2^{k_2})...(1 + p_r^1 + p_r^2 ... p_r^{k_r})$.
- Every term in the expansion of above product appears once and only once in $\sigma(n)$, so $\sigma(n)$ is equal to above product.

$\sigma(n)$

- By sum of finite geometrical series, we get $1+\mathrm{k}_1^1 + k_1^2 ... + k_1^r = \frac{p_1^{k_1+1}-1}{p_1-1}$.
- It follows that $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1}\frac{p_2^{k_2+1}-1}{p_2-1}...\frac{p_r^{k_r+1}-1}{p_r-1}$.

Observation

One interesting property of $\tau(n)$ is
$\prod_{d|n} d = n^{\tau(n)/2}$.

- Let d denote arbitrary divisor of n,such that n=dd'.
- We have $\tau(n)$ such equations and multiplying all of them we get $n^{\tau(n)} = \prod_{d|n} d \prod_{d'|n} d'$.
- As d runs over all divisors of n so does d',therefore $\prod_{d|n} d = \prod_{d'|n} d'$.
- Thus, $n^{\tau(n)} = (\prod_{d|n} d)^2$, or $\prod_{d|n} d = n^{\tau(n)/2}$.

Multiplicative Functions

Number theoretic functions are called multiplicative if
f(mn) = f(m)f(n) where gcd(m,n) = 1.

- Claim: $\tau(n)$ and $\sigma(n)$ are both multiplicative functions.
- Proof:
  If f is a multiplicative function which does not vanish identicaly, then there exist n such that f(n) $\neq$ 0.But, f(n) = f(n.1) = f(n)f(1).
  Canceling f(n) from both sides we get f(1) = 1.

- Let m,n are relatively prime integers. If $m = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ and n = $q_1^{j_1} q_2^{j_2} ... q_s^{j_s}$ and no p_i can occur among q_j.

Multiplicative Functions

- Now mn $= p_1^{k_1} p_2^{k_2} ... p_r^{k_r} q_1^{j_1} q_2^{j_2} ... q_s^{j_s}$.
- $\tau(mn) = [(k_1 + 1)(k_2 + 1)...(k_r + 1)][(q_1 + 1)(q_2 + 1)...(q_s + 1)]$.
  Thus, $\tau(n) = \tau(m)\tau(n)$.
- $\sigma(mn) = [\frac{p_1^{k_1+1}-1}{p_1-1}\frac{p_2^{k_2+1}-1}{p_2-1}...\frac{p_r^{k_r+1}-1}{p_r-1}][\frac{q_1^{j_1+1}-1}{q_1-1}\frac{q_2^{j_2+1}-1}{q_2-1}...\frac{q_r^{j_s+1}-1}{q_s-1}]$.
  Thus, $\sigma(mn) = \sigma(m)\sigma(n)$.

Mobius μ -function

For a positive integer n,
$\mu = 1$ if n = 1.
$\mu = 0$ if $p^2|n$ for some prime p.
$\mu = (-1)^r$ for $n = p_1 p_2 p_3 ... p_r$ where $p_i's$ are distinct primes.

- Theorem: μ is a multiplicative function.
- Proof:
  If there exist prime p such that $p^2|n$ or $p^2|m$ then $\mu(\text{mn}) = \mu(\text{m})\mu(\text{n})$ holds trivially. So we can assume m and n to square free integers. Let $m = p_1 p_2 ... p_r$ and $n = q_1 q_2 ... q_s$. the primes p_i and q_i being all distinct.
- Then $\mu(\text{mn}) = \mu(p_1 p_2 ... p_r q_1 q_2 ... q_s) = (\text{-}1)^{r+s} = (-1)^r(-1)^s$
  $= \mu(\text{m})\mu(\text{n})$, which completes the proof.

Mobius Inversion Formula

Mobius Inversion Formula: Let F and f are two number theoretic function related by the following relation

$F(n) = \Sigma_{d|n} f(d)$.

Then,

$f(n) = \Sigma_{d|n}\ \mu(d)F(n/d) = \Sigma_{d|n}\ \mu(n/d)F(d)$.

Proof:

The two sum mentioned in the above formula are seen to be the same upon replacing the dummy index d, by d' $=$ n/d. As d varies over all the positive divisors of n so does d'.

Proof

- $\Sigma_{d|n}\ \mu(\mathrm{d})\mathrm{F}(\mathrm{n}/\mathrm{d}) = \Sigma_{d|n}(\ \mu(\mathrm{d})\Sigma_{c|(n/d)}\mathrm{f}(\mathrm{c}))$
- It can be seen that d|n and c|(n/d) iff c| n and d|(n/c) .Then we have
- $\Sigma_{d|n}(\Sigma_{c|(n/d)}\mu(\mathrm{d})\mathrm{f}(\mathrm{c})) = \Sigma_{c|n}(\Sigma_{d|(n/c)}\mathrm{f}(\mathrm{c})\mu(\mathrm{d}))$
  $=\Sigma_{c|n}(\mathrm{f}(\mathrm{c})\Sigma_{d|(n/c)}\mu(\mathrm{d}))$
- The sum $\Sigma_{d|(n/c)}\mu(\mathrm{d})$ vanish except when n/c=1.
- $\Sigma_{c|n}(\mathrm{f}(\mathrm{c})\Sigma_{d|(n/c)}\mu(\mathrm{d})) = \Sigma_{c=n}\mathrm{f}(\mathrm{c}).1 = \mathrm{f}(\mathrm{n})$.

Observation

Theorem : If n is a positive integer and p a prime, then the exponent of highest power of p that divides n! is $\sum_{k=1}^{\infty}[n/p^k]$.
Proof: Among the first n positive integers,those which are divisible by p are p,2p,..,tp,where t is the largest integer such that tp$\leq$n or t = [n/p].Thus, there are exactly [n/p] multiples of p in the product that defines n!.
The exponent of p in the prime factorization of n! is obtained by adding to [n/p],the number of integers in 1,2,...,n divisible by p^2(which are by above reasoning $[n/p^2]$),and so on.
Thus, the total number of times p divides n! is $\sum_{k=1}^{\infty}[n/p^k]$.

$\phi(n)$

- $\phi(n)$,the number of positive integers not exceeding n and are relatively prime to n.
- $\phi(n)$,is also multiplicative function .
- If p is prime and k > 0, then $\phi(p^k) = p^k - p^{k-1}$
- For n > 2, ϕ(n) is an even integer .
- If n $= 2^k$, then ϕ(n) $= \phi(2^k) = 2^k(1 - 1/2) = 2^{k-1}$
- Otherwise, n $= p^k m$, where k ≥ 1 and gcd(p^k,m) $= 1$.
  ϕ(n) $= \phi(p^k)\phi$(m) $= p^{k-1}(p - 1)\phi$(m) wich is even as 2| p-1 .

Observation

For n > 1, the sum of the positive integers less then n and are relatively prime to n is $\frac{1}{2}n\phi(n)$.

- Let $\mathrm{a}_1, a_2, ..., a_{\phi(n)}$ be integers relatively prime to n.
- Now gcd(a,n) = 1 iff gcd(n-a,n) = 1 . Therefore numbers $\text{n-a}_1, n - a_2, ..., n - a_{\phi(n)}$ are equal in some order to $\mathrm{a}_1, a_2, ..., a_{\phi(n)}$.
- Thus,
  $\mathrm{a}_1 + a_2 + ... + a_{\phi(n)} = (\text{n-a}_1) + (n - a_2) + ... + (n - a_{\phi(n)})$
  $\mathrm{a}_1 + a_2 + ... + a_{\phi(n)} = \phi(n)\mathrm{n} - (\mathrm{a}_1 + a_2 + ... + a_{\phi(n)})$
- Hence, $\mathrm{a}_1 + a_2 + ... + a_{\phi(n)} = \frac{1}{2}n\phi(n)$

$\phi(n)$ in terms of $\mu - funtion$

For any positive integer n,

$$\phi(n) = \mathrm{n}\Sigma_{d|n} \ \frac{\mu(d)}{d}$$

- If we apply inversion formula to

  $\mathrm{F(n)} = \mathrm{n} = \Sigma_{d|n} \ \phi(d)$, we get
- $\phi(n) = \Sigma_{d|n}\mu(d)F(\frac{n}{d}) = \Sigma_{d|n}\mu(d)\frac{n}{d}$

For Further Reading I

David M. Burton.
Elementary Number Theory.

ThankYou!! Questions!!!