Apostol's Bag of Tricks

Stefanus[1]

[1] Samsung Semiconductor Inc

San Jose, CA 95134 USA

(Dated: August 5, 2017)

Abstract

Just for fun :)

1. **Page 158-159**, a delta function for Polynomial, *i.e.* $D_{z_m}(z) = 0$ if $z \neq z_m$ and $= 1$ only if $z = z_m$

$$D_{z_m}(z) = \frac{A_m(z)}{A_m(z_m)} \quad = \quad \begin{cases} 1 & \text{if } z = z_m \\ 0 & \text{otherwise} \end{cases}$$

where

$$A_m(z) = \frac{A(z)}{z - z_m} \qquad \text{with} \qquad A(z) = (z - z_0)(z - z_1)\ldots(z - z_{k-1})$$

2. Swapping dummy variables $n \to n = cd$

$$\sum_{n=1}^{k} \sum_{d|k, d|n} = \sum_{d|k} \sum_{c=1/d}^{k/d} = \sum_{d|k} \sum_{c=1}^{k/d}$$

going to the second inequality we need to swap the sums because now c is a function of d so d has to be defined before we can specify c, also $1/d$ starts with 1 because d starts with 1

3. swapping $d \leftrightarrow \frac{k}{d}$

$$\sum_{d|k} f(k) g\left(\frac{k}{d}\right) = \sum_{d|k} f\left(\frac{k}{d}\right) g(k)$$

as long as we sum over *all* divisors of k if we put another constraint we can't do the above

$$\sum_{d|(n,k)} f(k) g\left(\frac{k}{d}\right) \neq \sum_{d|(n,k)} f\left(\frac{k}{d}\right) g(k) \qquad \text{if } n \neq k$$

4. simplification on sums involving $\mu(d)$

$$\sum_{d|k} \mu(d) f(d) = \prod_{p|k} (1 - f(p))$$

as long as $f(n)$ is multiplicative, also $p|k$ only involves distinct p's, *i.e.* if $k = 100$ then the product is only for one copy of $p = 2$ and one copy of $p = 5$, $\prod_{p|100}(1 - f(p)) = (1 - f(2))(1 - f(5))$

5. For multiplicative functions

$$f(ab) = f(a)f(b) \qquad f(a) = \frac{f(ab)}{f(b} \qquad f(b) = \frac{f(ab)}{f(a)}$$

i.e. we can do "division" with them

6. Also for products involving "distinct" primes

$$\prod_{p|mk} f(p) = \prod_{p|m} f(p) \prod_{q|k} f(q) \qquad p \neq q$$

we can also do "division"

$$\prod_{p|m, p\nmid k} f(p) = \frac{\prod_{p|mk} f(p)}{\prod_{p|k} f(p)}$$

say $m = 6, k = 10$, $\prod_{p|6\cdot 10} f(p) = f(2)f(3)f(5)$, so we involve only distinct primes

7. Pigeon hole principle

8. $\int_1^x = \int_1^{\sqrt{x}} + \int_{\sqrt{x}}^x$, we might be able to get away with other powers, $x^{1/k}$, too

9. Consequences of being a finite group

   - if $a \in G$ then there is an $n \leq |G|$ such that $a^n = e$
   - for every subgroup G' of G, there is an indicator n of $a \in G$, such that $a^n \in G'$ this means that for $k < n$, $a^k \notin G'$
   - we can create a series of subgroups of G that has a nested structure, $G_1 \subset G_2 \subset \ldots G_{t+1} = G$ (Theorem 6.6 and 6.8), $G'' = \{xa^k : x \in G'$ and $k = 0, 1, 2, \ldots, h-1\}$ where h is the indicator of a in G'
   - the character $f(a)$ with $a \in G$, is just a root of unity because for some n, $a^n = e$
   - if G is abelian of order n there are exactly n characters

10. We can think of characters f_j of a finite abelian group as representations of the group since it's a one to one mapping, we can think of each character as a different representation although the main difference here is that we can take products of the characters, we can't take a product of different spins (different representations of $su(2)$)

11. Dirichlet's theorem is about distribution of primes, *i.e.* is it possible for an arithmetic progression $ak + b$ to contain no primes after certain point? The key is in using Dirichlet character $\sum \chi(n)f(n)$ because $\chi(n)$ is zero if n is not co-prime to k.

    This is actually in support of the randomness of primes, the probability of primes not hitting a single $ak + b$ will be really low if primes are random, because then it will have equal probability to hit any number

12. Dirichlet characters $\chi(n)$ modulo k can be perfectly played by the Legendre's symbols $\left(\frac{n}{k}\right)$ since

$$\left(\frac{n}{k}\right) = \begin{cases} +1 \text{ if } n \text{ is a quadratic residue modulo } k \\ -1 \text{ if } n \text{ is a nonquadratic residue modulo } k \\ \ \ 0 \ \text{ if } (n,k) > 1 \end{cases}$$

so the Legendre's symbols are roots of unity and they are zero if $(n, k) > 1$, also it satisfies the multiplicative and non-zero properties of characters

$$\left(\frac{ab}{k}\right) = \left(\frac{a}{k}\right)\left(\frac{b}{k}\right)$$
$$\left(\frac{n}{k}\right) \neq 0 \qquad \text{for } (n,k) = 1$$

and so we can replace the Dirichlet characters in the gauss sum with Legendre's symbols

$$G(n,\chi) = \sum_{m=1}^{k} \chi(m) e^{2\pi imn/k} \quad \longrightarrow \quad G(n,\chi) = \sum_{m=1}^{k} \left(\frac{m}{k}\right) e^{2\pi imn/k}$$

13. When summing over mod $\sum_{n \bmod k}$ we can extend the dummy variables

$$\sum_{m=1}^{k} f(m) = \sum_{m=1}^{k} f(am) \qquad \text{as long as } (a,k) = 1$$

14. Discrete delta function (non-normalized)

$$\sum_{m=1}^{k} e^{2\pi i m(n-d)/k} = k\delta_{n,d} \qquad \text{whenever } 0 \le n, d < k$$

Using the above two items we can prove the following, for separable gauss sums $|G(1,\chi)|^2 = k$, first

$$\begin{aligned} |G(n,\chi)|^2 &= |\overline{\chi}(n)G(1,\chi)|^2 \\ &= |\overline{\chi}(n)|^2 \, |G(1,\chi)|^2 \\ &= 1 \cdot |G(1,\chi)|^2 \end{aligned}$$

then

$$\begin{aligned} |G(1,\chi)|^2 = |G(n,\chi)|^2 &= \sum_{w=1}^{k} \overline{\chi}(w) e^{-2\pi i w n/k} \sum_{m=1}^{k} \chi(m) e^{2\pi i m n/k} \\ &= \sum_{w=1}^{k}\sum_{m=1}^{k} \chi(w^{-1})\chi(m) e^{2\pi i (m-w)n/k} \\ &= \sum_{w=1}^{k}\sum_{m=1}^{k} \chi(w^{-1}m) e^{2\pi i (m-w)n/k} \\ &= \sum_{w=1}^{k}\sum_{m=1}^{k} \chi(w^{-1}(wm)) e^{2\pi i (wm-w)n/k} \qquad \text{using item 13} \\ &= \sum_{w=1}^{k}\sum_{m=1}^{k} \chi(m) e^{2\pi i w(m-1)n/k} \\ &= \sum_{m=1}^{k} \chi(m) \sum_{w=1}^{k} e^{2\pi i w(m-1)n/k} \\ &= \sum_{m=1}^{k} \chi(m)\ k\ \delta_{m,1} \qquad \text{using item 14} \\ |G(1,\chi)|^2 &= k\ \chi(1) = k \end{aligned}$$

when using item 13 we multiply m by w but w runs from 1 to k and it's not always co-prime to k but this is all right since $\chi(wm) = 0$ if $(w,k) > 1$ and so the Dirichlet character took care of it

15. properties of gcd

$$(mk, ab) = (a, m)(k, b) \qquad \text{if } (a, k) = (b, m) = 1$$