Multiplicative Functions: NumThy

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
23 September, 2017 (at *15:50*)

Aside. In `number_theory.ams.tex` there is a bit more on multiplicative functions also in `mult.convolution.ams.tex`; run `collect.ams.tex` though.

See `generating_func.latex` for an application of the Möbius fnc.

Basic

Given two arbitrary[♡1] functions $f,g:\mathbb{Z}_+\to\mathbb{C}$, define their ***convolution*** ("Dirichlet convolution") by

$$\big[f\circledast g\big](K) \;:=\; \sum_{a\cdot b=K} f(a)\cdot g(b)\,.$$

Each such sum is to be interpreted as over all ordered pairs (a,b) of *positive* divisors of K. Easily, convolution is commutative[♡1] and associative.

Let $\widehat{\mathbb{G}}$ be the set of functions $f:\mathbb{Z}_+\to\mathbb{C}$ such that $f(1)\neq 0$. Inside is $\mathbb{G}\subset\widehat{\mathbb{G}}$, the set of ***good functions***, which have $f(1)=1$. Say that a good f is ***multiplicative*** if for all posints[♡2] K and Γ:

$$K\perp\Gamma \;\implies\; f(K\cdot\Gamma) \;=\; f(K)\cdot f(\Gamma)\,.$$

Let $\mathbb{M}\subset\mathbb{G}$ be the set of multiplicative[♡3] functions.

[♡1] Indeed, they could map into a general ring. If this ring is commutative then convolution will be commutative.

[♡2] Use $\equiv_N$ to mean "congruent mod N". Let $n\perp k$ mean that n and k are co-prime. Use $k\bullet\!|\, n$ for "k divides n". Its negation $k\not|\, n$ means "k does not divide n." Use $n\,|\!\bullet\, k$ and $n\not|\, k$ for "n is/is-not a multiple of k." Finally, for p a prime and E a natnum: Use double-verticals, $p^E\bullet\!\|\, n$, to mean that E is the ***highest*** power of p which divides n. Or write $n\,\|\!\bullet\, p^E$ to emphasize that this is an assertion about n. Use ***PoT*** for Power of Two and ***PoP*** for Power of (a) Prime.

For N a posint, use $\Phi(N)$ or Φ_N for the set $\{r\in[1\,..\,N]\mid r\perp N\}$. The cardinality $\varphi(N):=|\Phi_N|$ is the ***Euler phi function***. (So $\varphi(N)$ is the cardinality of the multiplicative group, Φ_N, in the $\mathbb{Z}_N$ ring.) Use ***EFT*** for the Euler-Fermat Thm, which says: *Suppose that integers $b\perp N$, with N positive. Then $b^{\varphi(N)}\equiv_N 1$.*

[♡3] An f is ***totally*** (or ***completely***) ***multiplicative*** if $f(K\cdot\Gamma)=f(K)\cdot f(\Gamma)$ always holds, even if $K\not\perp\Gamma$. This class is less important than $\mathbb{M}$. Indeed, the set of *totally* multiplicative fncs is **not** sealed under convolution.

Basic functions. Define fncs $\delta,\mathbf{1},Id\in\mathbb{M}$ by:

$$\begin{aligned}\delta(1)&:=1 \quad\text{and}\quad \delta(\neq 1):=0\,;\\ \mathbf{1}(n)&:=1 \quad\text{and}\\ Id(n)&:=n \quad\text{for all posints } n.\end{aligned}$$

Evidently $\delta()$ is a neutral element for convolution.

Also define, as n varies over the posints, these MFs:

$$\begin{aligned}\boldsymbol{\tau}(n)&:=\sum\nolimits_{d:d\bullet\!|n} 1 \quad\text{and}\\ \boldsymbol{\sigma}(n)&:=\sum\nolimits_{d:d\bullet\!|n} d\,.\end{aligned}$$

This $\boldsymbol{\tau}$ is called the (number of) ***divisor*** function, and $\boldsymbol{\sigma}$ is called the ***sum of divisor*** fnc. E.g, $\boldsymbol{\sigma}(4)=1+2+4=7$ and $\boldsymbol{\tau}(4)=1+1+1=3$.

Each of $\delta,\mathbf{1},Id,\boldsymbol{\tau},\boldsymbol{\sigma}$ is multiplicative. So is Euler $\boldsymbol{\varphi}$; this will follow from (4).

1: Theorem. *$(\widehat{\mathbb{G}},\circledast,\delta)$ is a commutative group and $\mathbb{M}\subset\mathbb{G}\subset\widehat{\mathbb{G}}$ are subgroups.* ◊

Pf. To see that δ is a $\circledast$-identity-elt on $\widehat{\mathbb{G}}$, note $\big[f\circledast Id\big](K)=\sum_{a\cdot b=K} f(a)\cdot\delta(b)=f(K)\cdot\delta(1)\overset{\text{note}}{=\!=}f(K)$.

(The below arguments showing $\mathbb{G}$ a group apply to show $\widehat{\mathbb{G}}$ a group. So we only argue for $\mathbb{G}$ and $\mathbb{M}$.)

Easily $\mathbb{G}$ is sealed under convolution. To show the same for $\mathbb{M}$, take fncs $f,h\in\mathbb{M}$ and posints $K\perp\Gamma$. Given posints (x,y) with $x\cdot y$ equaling the product $K\Gamma$, the FTArithm says that we can factor uniquely $x=a\alpha$ and $y=b\beta$ into posints so that $a,b\bullet\!|\, K$ and $\alpha,\beta\bullet\!|\,\Gamma$. Thus

1a:
$$\begin{aligned}\big[f\circledast h\big](K\Gamma) \;&=\; \sum_{x\cdot y=K\Gamma} f(x)h(y)\\ &=\; \sum_{\substack{a\cdot b=K\\ \alpha\cdot\beta=\Gamma}} f(a\alpha)h(b\beta)\,.\end{aligned}$$

Necessarily $a \perp \alpha$ and $b \perp \beta$, since $K \perp \Gamma$. Since f and h are each multiplicative fncs,

$$\Big[f \circledast h\Big](K\Gamma) \;=\; \sum_{\substack{a\cdot b=K\\ \alpha\cdot\beta=\Gamma}} f(a)f(\alpha)h(b)h(\beta)$$

1b:

$$= \Big[\sum_{a\cdot b=K} f(a)h(b)\Big]\cdot\Big[\sum_{\alpha\cdot\beta=\Gamma} f(\alpha)h(\beta)\Big]\,.$$

And this last equals $\Big[f \circledast h\Big](K)$ times $\Big[f \circledast h\Big](\Gamma)$.

Each good f has a convolution inverse. We construct an $h \in \mathbb{G}$ so that $f \circledast h = \delta$. For each posint K, then,

$$\delta(K) \;=\; f(1)\cdot h(K) + \sum_{\substack{a\cdot b=K\\ (a,b)\neq(1,K)}} f(a)\cdot h(b)\,.$$

Since $f(1)$=1 is not zero, there is a unique value that we can assign $h(K)$ so as to make the displayed-eqn hold. Finally note that $h(1)$ will indeed be assigned the value 1, so h is good. This shows that $\mathbb{G}$ is a group.

$\mathbb{M}$ is sealed under convolution-inverse. The last step –to showing that $(\mathbb{M}, \circledast, \delta)$ is a group– is to show that when the above f is multiplicative, then the corresponding h is too.

An inductive proof that $h(K\Gamma) = h(K)h(\Gamma)$ proceeds by considering a pair $K\perp\Gamma$ for which

1c: $h(b\beta) = h(b)h(\beta)$ *for each* ***proper*** *divisor pair* (b,β) $\bullet\!\!|$ (K,Γ).

That is, $b \bullet\!\!| K$ and $\beta \bullet\!\!| \Gamma$ with at least one of these being proper.

Now WLOG $(K,\Gamma) \neq (1,1)$, so $\delta(K\Gamma) = 0$, i.e $[f \circledast h](K\Gamma)$ is zero. Hence

$$0 \;=\; \sum_{\substack{a\cdot b=K\\ \alpha\cdot\beta=\Gamma}} f(a\alpha)h(b\beta)$$

$$= \Big[\sum_{\substack{a\cdot b=K,\\ \alpha\cdot\beta=\Gamma,\\ (b,\beta)\neq(K,\Gamma)}} f(a\alpha)h(b\beta)\Big] \;+\; f(1\cdot1)\cdot h(K\Gamma)\,.$$

As $f(1\cdot1)$ equals 1, we can write

$$*\text{:}\qquad -h(K\Gamma) \;=\; \Big[\sum_{\substack{a\cdot b=K,\\ \alpha\cdot\beta=\Gamma,\\ (b,\beta)\neq(K,\Gamma)}} f(a\alpha)\cdot h(b)h(\beta)\Big]\,,$$

since, by (1c), our h is multiplicative on all the (b,β) pairs on RhS$(*)$. Adding $f(1\cdot1)h(K)h(\Gamma)$ to each side [again using that $f(1\cdot1)=1$], gives

$$h(K)h(\Gamma) - h(K\Gamma) \;=\; \sum_{\substack{a\cdot b=K,\\ \alpha\cdot\beta=\Gamma}} f(a\alpha)\cdot h(b)h(\beta)\,.$$

Since f is multiplicative, this RhS equals

$$\Big[\sum_{a\cdot b=K} f(a)h(b)\Big]\cdot\Big[\sum_{\alpha\cdot\beta=\Gamma} f(\alpha)h(\beta)\Big]$$

$$\stackrel{\text{def}}{=\!=} [f\circledast h](K)\cdot[f\circledast h](\Gamma) \;=\; \delta(K)\delta(\Gamma)\,.$$

Putting it all together,

$$**\text{:}\qquad h(K)h(\Gamma) - h(K\Gamma) \;=\; \delta(K\cdot\Gamma)\,,$$

since $\delta()$ is a MF. Finally, RhS$(**)$ is zero, since $K\cdot\Gamma \neq 1$. ♦

2: Lemma. *Suppose that f and g are MFs. Then $f\cdot g$ (pointwise product) is a MF. If g is nowhere zero, then ptwise quotient f/g is a MF.*
Proof. Routine. ◊

Analogy. Recall that CRThm allows us to convert polynomial congruences $f(x) \equiv 0$ modulo a composite M to just examining $f(x) \equiv 0$ modulo p^L; we only need consider powers of primes.

In analogy, the MF theory allows us to convert proving an identity $h() = g()$, between MFncs, on *all* of $\mathbb{Z}_+$, to just verifying it on each prime-power p^L. □

Applications

Define the ***Möbius fnc*** $\boldsymbol{\mu}$ to be the *convolution-inverse of* $\mathbf{1}$. I.e $\boxed{\boldsymbol{\mu} := \mathbf{1}^{\circledast -1}}$, so $\boldsymbol{\mu}$ is characterized by $\boldsymbol{\mu} \circledast \mathbf{1} = \delta$. By Thm 1, it is enough to know $\boldsymbol{\mu}()$'s values on the powers of primes.

3: Lemma. *For each prime p and exponent n in $[2\,..\,\infty)$:*

$$\boldsymbol{\mu}(p) = -1 \quad \text{and} \quad \boldsymbol{\mu}(p^n) = 0\,. \qquad \Diamond$$

Proof. Well $0 = \delta(p) = \boldsymbol{\mu}(p) + \boldsymbol{\mu}(1) = \boldsymbol{\mu}(p) + 1$.
For a higher power of p:

$$0 = \delta(p^n) = \boldsymbol{\mu}(1) + \boldsymbol{\mu}(p) + S + \boldsymbol{\mu}(p^n)\,,$$

where $S := \sum_{j=2}^{n-1} \boldsymbol{\mu}(p^j)$. This S, by induction, is zero. Thus $\boldsymbol{\mu}(p^n) = -\big[\boldsymbol{\mu}(1) + \boldsymbol{\mu}(p)\big]$, which is zero. ♦

Before developing further results, note that:

For each good f, necessarily $f^{\circledast 0} = \delta$,

since δ is the neutral element for $\circledast$. We now need a little tool.

4: Bijection Lemma. *Fixing a posint N, let $g(\ell)$ mean $\mathrm{Gcd}\{\ell, N\}$. Then there is a bijection*

$$\text{a:}\quad [1\,..\,N] \hookrightarrow \bigsqcup_{d:d\,|\,N} \Phi(d)\times\{d\} \overset{\text{note}}{=\!=} \left\{ \boldsymbol{(}x, d\boldsymbol{)} \;\middle|\; \begin{smallmatrix} d\,|\,N \\ \text{and} \\ x\in\Phi(d) \end{smallmatrix} \right\}$$

realized by the mapping

$$\text{b:}\qquad \ell \mapsto \boldsymbol{(}x_\ell, d_\ell\boldsymbol{)}\,, \quad \text{where} \quad \begin{smallmatrix} x_\ell \coloneqq \ell/g(\ell) \ \text{ and} \\ d_\ell \coloneqq N/g(\ell) \end{smallmatrix}$$

The inverse bijection is

$$\text{c:}\qquad \boldsymbol{(}x, d\boldsymbol{)} \mapsto x\cdot\tfrac{N}{d}\,. \qquad \Diamond$$

We now establish a few useful relations.

5: Basic Lemma. *Among MFs $\mathbf{1}, \boldsymbol{\tau}, \boldsymbol{\sigma}, Id, \boldsymbol{\mu}$ and $\boldsymbol{\varphi}$, the following relations hold.*

i: $\mathbf{1} \circledast \mathbf{1} = \boldsymbol{\tau}$. *Also* $Id \circledast \mathbf{1} = \boldsymbol{\sigma}$, *so* $Id = \boldsymbol{\sigma} \circledast \boldsymbol{\mu}$.

ii: $\boldsymbol{\mu} \circledast \mathbf{1} = \delta$.

iii: $\boldsymbol{\varphi} \circledast \mathbf{1} = Id$.

iv: $\boldsymbol{\varphi} \circledast \boldsymbol{\tau} = \boldsymbol{\sigma}$ *and* $\boldsymbol{\varphi} \circledast \boldsymbol{\sigma} = Id^{\circledast 2}$. $\Diamond$

Proof of iii. Take cardinalities in (4a), which gives $Id = \boldsymbol{\varphi} \circledast \mathbf{1}$. As for (iv), note that

$$\boldsymbol{\varphi} \circledast \boldsymbol{\tau} = \boldsymbol{\varphi} \circledast \mathbf{1} \circledast \mathbf{1} = Id \circledast \mathbf{1}\,,$$

which is $\boldsymbol{\sigma}$, by definition. ♦

6: Prop'n. *The fnc $\boldsymbol{\varphi}/Id$ is multiplicative. And*

$$\text{a,b:}\quad \limsup_{K\to\infty} \tfrac{\varphi(K)}{K} = 1 \quad \text{and} \quad \liminf_{K\to\infty} \tfrac{\varphi(K)}{K} = 0\,.$$

$$\text{c:}\quad \text{Finally,} \quad \varphi(K) \to \infty \quad \text{as} \quad K \nearrow \infty\,. \qquad \Diamond$$

Proof. Exercise. ♦

Convolution powers. Using binomial coefficients, [♡4] one can show that

$$\mathbf{1}^{\circledast n}(p^L) = \binom{L+n-1}{L}\,,$$

[♡4] For a natnum n, use "$n!$" to mean "n ***factorial***"; the product of all positive-integers less-equal n. So $3! = 3\cdot 2\cdot 1 = 6$ and $5! = 120$. Also $0! = 1$ and $1! = 1$.

The ***binomial coefficient*** $\binom{7}{3}$, read "7 choose 3", means *the number of ways of choosing* 3 *objects from* 7 *distinguishable objects.* If we think of putting these objects in our left pocket, and putting the remaining 4 things in our right pocket, then we write the coefficient as $\binom{7}{3,4}$. [Read as "7 choose 3-comma-4."] Note that $\binom{7}{0} = \binom{7}{0,7} = 1$. Also note this identity:

$$[x+y]^N = \sum_{j+k=N} \tbinom{N}{j,k} \cdot x^j y^k\,,$$

where $\boldsymbol{(}j, k\boldsymbol{)}$ ranges over all *ordered* pairs of natural numbers with sum N.

In general, for natnums $N = K_1 + \ldots + K_L$, the ***multinomial coefficient*** $\binom{N}{K_1, K_2, \ldots, K_L}$ means the number of ways of partitioning N different things, by putting K_1 of them in pocket 1 and K_2 of them in pocket 2, and so on. Easily

$$\binom{N}{K_1, K_2, \ldots, K_L} = \frac{N!}{K_1!\cdot K_2! \cdots K_L!}\,.$$

for each prime p. Furthermore

$$\boldsymbol{\mu}^{\circledast n}(p^L) \;=\; [\text{-}1]^L \cdot \binom{n}{L}.$$

These are routinely proved by induction on n.

Applications of Möbius Inversion

An N^{th}-root ω of unity is ***primitive*** if, for each k in $[1\,..\,N)$, this ω is *not* a k^{th}-root of unity. Use $\mathbf{V}_N$ for the set of primitiVe N^{th}-roots. Define the "***N^{th} cyclotomic polynomial***" by

7a: $$\mathbf{C}_N(z) \;:=\; \prod_{\omega\in\mathbf{V}_N} [z-\omega]\,.$$

Letting $F_N(z) := z^N - 1$, note that

7b: $$F_N(x) \;=\; \prod_{d\bullet|N} \mathbf{C}_d(x)\,.$$

Used recursively, we compute these cyclo-polys:

7c: Examples:

$\mathbf{C}_1(z) = z-1$; $\mathbf{C}_3(z) = z^2+z+1$; $\mathbf{C}_5(z) = z^4+z^3+z^2+z+1$;
$\mathbf{C}_2(z) = z+1$; $\mathbf{C}_4(z) = z^2+1$; $\mathbf{C}_6(z) = z^2-z+1$.

8: Prop'n. *The sum of all the N^{th}-roots of unity equals $\delta(N)$. And their product is $[\text{-}1]^{N+1}$.*
The sum of all primitive N^{th}-roots equals $\boldsymbol{\mu}(N)$. Their product is 1, except when $N=2$ where the product is -1. ♢

Pf for all roots. Let S be the sum[♡5], and P the product, of the set, $\mathbf{A}$, of all N^{th}-roots. Thus

$$x^N - S{\cdot}x^{N-1} + \cdots + [\text{-}1]^N{\cdot}P \;=\; \prod_{Z\in\mathbf{A}} [x-Z] \;=\; x^N - 1. \;♦$$

And $[x_1+\cdots+x_L]^N$ indeed equals the sum of

$$\binom{N}{K_1,\ldots,K_L}\cdot {x_1}^{K_1}\cdot {x_2}^{K_2}\cdots {x_L}^{K_L}\,,$$

taken over all natnum-tuples $\vec{K}=(K_1,\ldots,K_L)$ that sum to N.

[♡5]For the sum, an alternative proof is to fix a primitive N^{th} root ω. Now $S_N := \sum_{k=0}^{N-1}\omega^k$ is the sum of all N^{th} roots. So $S_1 = 1 = \delta(1)$. For $N\in[2\,..\,\infty)$, note $\omega\neq 1$ so $S_N = \frac{\omega^N-1}{\omega-1} = 0 = \delta(N)$.

Pf for primitive roots. Let $S(n) := \sum(\mathbf{V}_n)$. Summing over the (positive) divisors $a \bullet| N$ gives

$$\sum_{a\cdot b=N} S(a) \;=\; \left[\begin{smallmatrix}\text{Sum of all}\\ N^{\text{th}}\text{ roots}\end{smallmatrix}\right] \;=\; \delta(N)\,.$$

IOWords, $S \circledast \mathbf{1} = \delta$. Thus $S = \delta \circledast \boldsymbol{\mu} = \boldsymbol{\mu}$.

As for the product, non-real primroots come in conjugate pairs. Each conjugate pair multiplies to 1. So $\sum(\mathbf{V}_N)$ is 1 *–unless* [-1] is an N^{th} primroot, which happens exactly when $N=2$. ♦

Defn. For a poly with non-zero constant term, e.g $g(x) := 9x^3+8x-6$, its ***reversal*** $\overleftarrow{g}$ has the coeffs in reverse order. So $\overleftarrow{g}(x) = \text{-}6x^3+8x^2+9$. □

9: Lemma. *Each $\mathbf{C}_N$ is a monic intpoly, of degree $|\mathbf{V}_N| \overset{\text{note}}{=\!=} \varphi(N)$. When $N\in[2\,..\,\infty)$, moreover, $\mathbf{C}_N$ is **palindromic** in that $\overleftarrow{\mathbf{C}_N} = \mathbf{C}_N$.*
Finally, for $N\geqslant 2$ and $K := \varphi(N)$,

9a: $$\mathbf{C}_N(x) \;=\; x^K - \boldsymbol{\mu}(N)x^{K-1} + \cdots + [\text{-}\boldsymbol{\mu}(N)]x + 1\,.\;♢$$

Proof. Equation (7b) gives

$$\mathbf{C}_N \;=\; F_N \Big/ \prod_{\substack{d\bullet|N\\ d\neq N}} \mathbf{C}_d\,.$$

By induction on N, each of the $\mathbf{C}_d$ is a monic intpoly. And easily: *If a monic intpoly divides another, then the quotient is a monic intpoly.*

Reversal. Consider a $Z\in\mathbf{V}_N$. Algebra gives

$$x{\cdot}[\tfrac{1}{x} - Z] \;=\; \text{-}1{\cdot}[xZ-1] \;=\; \text{-}1{\cdot}Z{\cdot}[x-\tfrac{1}{Z}]\,.$$

Now $\overleftarrow{\mathbf{C}_N}(x)$ equals $x^K{\cdot}\,\mathbf{C}_N(\frac{1}{x})$ which equals

$$\prod_{Z\in\mathbf{V}_N} x\cdot[\tfrac{1}{x}-Z] \;=\; [\text{-}1]^K \cdot \Big[\prod_{Z\in\mathbf{V}_N} Z\Big]\cdot \prod_{Z\in\mathbf{V}_N}[x-\tfrac{1}{Z}]\,.$$

Since $\mathbf{C}_2(x)=[x+1]$ is palindromic, WLOG $N\geqslant 3$. Thus $K := \varphi(N)$ is even. Also, (8) says that $\left[\prod_{Z\in\mathbf{V}_N} Z\right] = 1$. Thus

$$\overleftarrow{\mathbf{C}_N}(x) \;=\; 1\cdot 1\cdot \prod_{Z\in\mathbf{V}_N}[x-\tfrac{1}{Z}] \;\overset{\text{note}}{=\!=}\; \mathbf{C}_N(x)\,.$$

Lastly, (9a) follows from (8). ♦

10: Theorem. *Each* $\mathbf{C}_N$ *can be described by inclusion-exclusion as:*

$$\mathbf{C}_N(z) \;=\; \prod_{a\cdot b=N} [z^a-1]^{\boldsymbol{\mu}(b)} \overset{\text{note}}{=\!=} \prod_{a\cdot b=N} \mathbf{C}_1(z^a)^{\boldsymbol{\mu}(b)}$$

11:
$$\overset{\text{note}}{=\!=} \prod_{\substack{a\cdot b=N\,,\text{ with}\\ b\text{ square-free}}} \mathbf{C}_1(z^a)^{\boldsymbol{\mu}(b)}.$$

Below: P *is prime,* Γ *and* N *are posints and* K *a natnum.*

11i: *Now suppose* $P\perp\Gamma$. *Then*

$$\mathbf{C}_{P^{K+1}\Gamma}(z) \;=\; \mathbf{C}_\Gamma(z^{P^{K+1}})\big/\mathbf{C}_\Gamma(z^{P^K})\,.$$

In particular, setting $\Gamma:=1$,

$$\mathbf{C}_{P^{K+1}}(z) \;=\; \frac{[z^{P^K}]^P-1}{[z^{P^K}]-1} \;=\; \mathbf{C}_P(z^{P^K})\,.$$

11ii: *Consider an* $N\perp\Gamma$. *Then*

$\dagger_N$: $$\mathbf{C}_{N\Gamma}(z) \;=\; \prod_{a\cdot b=N} \mathbf{C}_\Gamma(z^a)^{\boldsymbol{\mu}(b)}$$

This generalizes (11). ♢

Pf of (i). Set $L:=K{+}1$ and apply (11) to $N:=P^L\Gamma$. Omitting all pairs $a{\cdot}b{=}N$ with $b\nmid P^2$ means that a has form either αP^L or αP^K. So

$$\begin{aligned}\mathbf{C}_N \;&=\; \Big[\prod_{\alpha P^L\cdot\beta=N}[F_{\alpha P^L}]^{\boldsymbol{\mu}(\beta)}\Big]\cdot\Big[\prod_{\alpha P^K\cdot P\beta=N}[F_{\alpha P^K}]^{\boldsymbol{\mu}(P\beta)}\Big]\\ &=\; \prod_{\alpha\cdot\beta=\Gamma}[F_{\alpha P^L}]^{\boldsymbol{\mu}(\beta)}\Big/\prod_{\alpha\cdot\beta=\Gamma}[F_{\alpha P^K}]^{\boldsymbol{\mu}(\beta)}\,.\end{aligned}$$

I.e $\mathbf{C}_N(z) \;=\; \mathbf{C}_\Gamma(z^{P^L})/\mathbf{C}_\Gamma(z^{P^K})$. ♦

Aside. Letting $R:=P^L$, we can restate the above conclusion as

‡: $$\mathbf{C}_{R\Gamma}(z) \;=\; \prod_{i\cdot j=R} \mathbf{C}_\Gamma(z^i)^{\boldsymbol{\mu}(j)}\,.$$ □

Pf of (ii). Whoa! This proof, while correct, should be rewritten

Eqn ($\dagger_1$) is a tautology. So, given $M\perp\Gamma$, we'll establish ($\dagger_M$) by induction on the number of PoPs in M. Write $M=NR$ with R a PoP co-prime to N. Then $\mathbf{C}_{M\Gamma}(z)$ equals

$$\begin{aligned}\mathbf{C}_{NR\Gamma}(z) \;&\overset{\text{by }(\dagger_N)}{=\!=} \prod_{a\cdot b=N}\mathbf{C}_{R\Gamma}(z^a)^{\boldsymbol{\mu}(b)}\\ &\overset{\text{by }(\ddagger)}{=\!=} \prod_{a\cdot b=N}\Big[\prod_{i\cdot j=R}\mathbf{C}_\Gamma\Big([z^a]^i\Big)^{\boldsymbol{\mu}(j)}\Big]^{\boldsymbol{\mu}(b)}\\ &=\; \prod_{\substack{a\cdot b=N\\ i\cdot j=R}}\mathbf{C}_\Gamma(z^{ai})^{\boldsymbol{\mu}(bj)}\,.\end{aligned}$$

This, since $b\perp j$, because $N\perp R$. Letting $x:=ai$ and $y:=bj$, the co-primeness $N\perp R$ again gives

$$\mathbf{C}_{M\Gamma}(z) \;=\; \prod_{x\cdot y=NR}\mathbf{C}_\Gamma(z^x)^{\boldsymbol{\mu}(y)}\,.$$ ♦

Filename: `Problems/NumberTheory/multiplicative_fncs.latex`
As of: *Monday 26May2003.* Typeset: *23Sep2017 at 15:50.*