Multiplicative Functions: NumThy

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
11 July, 2018 (at *17:20*)

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

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

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 $k\bullet\!\!\mid n$ for "k divides n". Its negation $k\not\bullet\!\!\mid n$ means "k does not divide n." Use $n\mid\!\!\bullet\, k$ and $n\not\mid\!\!\bullet\, k$ 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.] Easily, $\varphi(p^L)=[p-1]\cdot p^{L-1}$, for prime p and posint L.

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:

$$\delta(1):=1 \quad \textit{and} \quad \delta(\neq 1):=0\,;$$
$$\mathbf{1}(n):=1 \quad \textit{and}$$
$$Id(n):=n\,.$$

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

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

$$\boldsymbol{\tau}(n) \;:=\; \sum_{d:d\bullet\!\!\mid n} 1 \quad \textit{and}$$
$$\boldsymbol{\sigma}(n) \;:=\; \sum_{d:d\bullet\!\!\mid n} d\,. \quad \textit{Generalizing}$$
$$\boldsymbol{\sigma}_\alpha(n) \;:=\; \sum_{d:d\bullet\!\!\mid n} d^{\,\alpha}, \quad \textit{for } \alpha\in\mathbb{C}.$$

This $\boldsymbol{\tau}$ is called the ***divisor-count*** function, and $\boldsymbol{\sigma}$ is called the ***divisor-sum*** fnc. E.g, $\boldsymbol{\sigma}(4)=1+2+4=7$ and $\boldsymbol{\tau}(4)=1+1+1=3$. Note that $\boldsymbol{\sigma}_0=\boldsymbol{\tau}$ and $\boldsymbol{\sigma}_1=\boldsymbol{\sigma}$. Also...

1: *Each of $\delta,\mathbf{1},Id,\boldsymbol{\tau},\boldsymbol{\sigma}_\alpha$ is multiplicative.*

Exer 1: Use the uniqueness part of FTArithmetic to prove $\boldsymbol{\tau}$ multiplicative. [Same argument applies to $\boldsymbol{\sigma}_\alpha$.]

2: Theorem. *For prime p and natnum L:*

2a: $$\boldsymbol{\tau}(p^L) \;=\; L+1\,.$$

2b: *For $\alpha\neq 0$:* $$\boldsymbol{\sigma}_\alpha(p^L) \;=\; \frac{p^{[L+1]\alpha}\;-\;1}{p^\alpha\;-\;1}\,.$$

Proof. Exercise 2. ♢

Defn and EFT. 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.] Easily, $\varphi(p^L)=[p-1]\cdot p^{L-1}$, for prime p and posint L.

Use ***EFT*** for the Euler-Fermat Thm, which says: *Suppose that integers $b\perp N$, with N positive. Then $b^{\varphi(N)}\equiv_N 1$.*

Euler φ is multiplicative; this will follow from (7).□

3: 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 $[f \circledast Id](K) = \sum_{a\cdot b=K} f(a)\cdot\delta(b) = f(K)\cdot\delta(1) \overset{\text{note}}{=\!=} f(K)$.

(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 $\mathbf{(}x, y\mathbf{)}$ 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

3a:
$$\begin{aligned}[f \circledast h](K\Gamma) &= \sum_{x\cdot y = K\Gamma} f(x)h(y) \\ &= \sum_{\substack{a\cdot b = K \\ \alpha\cdot\beta=\Gamma}} f(a\alpha)h(b\beta)\,.\end{aligned}$$

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

3b:
$$\begin{aligned}[f \circledast h](K\Gamma) &= \sum_{\substack{a\cdot b=K \\ \alpha\cdot\beta=\Gamma}} f(a)f(\alpha)h(b)h(\beta) \\ &= \Big[\sum_{a\cdot b=K} f(a)h(b)\Big]\cdot\Big[\sum_{\alpha\cdot\beta=\Gamma} f(\alpha)h(\beta)\Big]\,.\end{aligned}$$

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

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,

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

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 $\mathbf{(}\mathbb{M}, \circledast, \delta\mathbf{)}$ 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

3c: *$h(b\beta) = h(b)h(\beta)$ for each **proper** divisor pair $\mathbf{(}b, \beta\mathbf{)} \bullet\!| \mathbf{(}K, \Gamma\mathbf{)}$.*

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

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

$$\begin{aligned}0 &= \sum_{\substack{a\cdot b=K \\ \alpha\cdot\beta=\Gamma}} f(a\alpha)h(b\beta) \\ &= \Big[\sum_{\substack{a\cdot b=K, \\ \alpha\cdot\beta=\Gamma, \\ \mathbf{(}b,\beta\mathbf{)}\neq\mathbf{(}K,\Gamma\mathbf{)}}} f(a\alpha)h(b\beta)\Big] + f(1\cdot1)\cdot h(K\Gamma)\,.\end{aligned}$$

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

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

since, by (3c), our h is multiplicative on all the $\mathbf{(}b, \beta\mathbf{)}$ 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

$$\begin{aligned}&\Big[\sum_{a\cdot b=K} f(a)h(b)\Big]\cdot\Big[\sum_{\alpha\cdot\beta=\Gamma} f(\alpha)h(\beta)\Big] \\ &\overset{\text{def}}{=\!=} [f \circledast h](K)\cdot[f \circledast h](\Gamma) = \delta(K)\delta(\Gamma)\,.\end{aligned}$$

Putting it all together,

$**$:
$$h(K)h(\Gamma) - h(K\Gamma) = \delta(K\cdot\Gamma)\,,$$

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

4: Lemma. *Suppose that f and g are MFs. Then $f\cdot g$ (pointwise product) is a MF. If g is no-where 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 <u>all</u> 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 3, it is enough to know $\boldsymbol{\mu}()$'s values on the powers of primes.

5: 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 $\boldsymbol{\mu}(p^n) = -[\boldsymbol{\mu}(1) + \boldsymbol{\mu}(p)]$, 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.

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

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

realized by the mapping

b: $$\ell \mapsto (x_\ell, d_\ell)\,, \quad \text{where} \quad \begin{array}{l} x_\ell \coloneqq \ell / g(\ell) \;\text{ and} \\ d_\ell \coloneqq N / g(\ell) \end{array}$$

The inverse bijection is

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

We now establish a few useful relations.

7: 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 (6a), 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. ♦

7a: Coro. *Euler $\boldsymbol{\varphi}$ is multiplicative.* $\Diamond$

Proof. Courtesy (7iii), $\boldsymbol{\varphi} = Id \circledast \mathbf{1}$ is a convolution of MFs, hence is an MF itself, by (3). ♦

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

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

c: *Finally,* $\boldsymbol{\varphi}(K) \to \infty$ *as* $K \nearrow \infty$. $\Diamond$

Pf of (a). On primes, $\frac{\boldsymbol{\varphi}(p)}{p} = \frac{p-1}{p} = 1 - \frac{1}{p}$. Etc. ♦

Pf of (b). Let K_n be the product of the first n primes. Exer 3. Now... ? ♦

Pf of (c). FTSOC, imagine a seq. $K_1 < K_2 < \ldots$ along which $\boldsymbol{\varphi}()$ stays bounded. Prove there is a bound –say, 100– so that for all primes p and all j: If p^L is in the pop-decomp of K_j, then $L \leqslant 100$. Exer 4. Now... ? ♦

Convolution powers. Using binomial coefficients [reviewed in Appendix A, P.6], one can show that

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

for each prime p. Furthermore

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

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

9a: $$\mathbf{C}_N(z) \;:=\; \prod_{\omega\in\mathbf{V}_N} [z-\omega]\,.$$

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

9b: $$F_N(x) \;=\; \prod_{d\,|\,N} \mathbf{C}_d(x)\,.$$

Used recursively, we compute these cyclo-polys:

9c: Examples:

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

10: Prop'n. *The sum of all the N^{th}-roots of unity equals $\delta(N)$. And their product is $[-1]^{N+1}$.*

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[♡4], and P the product, of the set, $\mathbf{A}$, of all N^{th}-roots. Thus

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

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

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

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 $\overleftarrow{g}(x) = -6x^3+8x^2+9$. □

[♡4] 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 $S_N = \frac{\omega^N-1}{\omega-1} = 0 = \delta(N)$.

11: Lemma. *Each $\mathbf{C}_N$ is a monic intpoly, of degree $|\mathbf{V}_N| \overset{\text{note}}{=\!=} \boldsymbol{\varphi}(N)$. 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 $K := \boldsymbol{\varphi}(N)$,

11a: $$\mathbf{C}_N(x) \;=\; x^K - \boldsymbol{\mu}(N)x^{K-1} + \cdots + [-\boldsymbol{\mu}(N)]x + 1\,. \quad ♢$$

Proof. Equation (9b) gives

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

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

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

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

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

Since $\mathbf{C}_2(x)=[x+1]$ is palindromic, WLOG $N\geqslant 3$. Thus $K := \boldsymbol{\varphi}(N)$ is even. Also, (10) says that $[\prod_{Z\in\mathbf{V}_N} Z] = 1$. 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, (11a) follows from (10). ♦

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

13:
$$\mathbf{C}_N(z) \;=\; \prod_{a\cdot b=N} [z^a-1]^{\boldsymbol{\mu}(b)} \overset{\text{note}}{=\!=} \prod_{a\cdot b=N} \mathbf{C}_1(z^a)^{\boldsymbol{\mu}(b)} \overset{\text{note}}{=\!=} \prod_{\substack{a\cdot b=N\,,\text{ with}\\ b\text{ square-free}}} \mathbf{C}_1(z^a)^{\boldsymbol{\mu}(b)}.$$

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

13i: *Now suppose $P \perp \Gamma$. Then*

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

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

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

13ii: *Consider an* $N \perp \Gamma$. *Then*

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

This generalizes (13). ◊

Pf of (i). Set $L := K{+}1$ and apply (13) to $N := P^L\Gamma$. Omitting all pairs $a{\cdot}b{=}N$ with $b \not\bullet P^2$ 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

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

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

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

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

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

§A Appendix

A For a natnum n, use "$n!$" to mean "***n factorial***"; the product of all posints $\leqslant n$. So $3! = 3 \cdot 2 \cdot 1 = 6$ and $5! = 120$. Also $0! = 1$ and $1! = 1$.

For natnum j and arb. complex number β, define

$$[\![\beta \downarrow j]\!] \;:=\; \beta \cdot [\beta - 1] \cdot [\beta - 2] \cdot \ldots \cdot [\beta - [j{-}1]] \,;$$

this is read as "β ***falling factorial*** j". E.g,

$$\left[\!\!\left[\tfrac{2}{7} \;\middle\downarrow\; 4 \right]\!\!\right] = \frac{2}{7} \cdot \frac{-5}{7} \cdot \frac{-12}{7} \cdot \frac{-19}{7} \text{ and } [\![1 \downarrow 3]\!] = 1 \cdot 0 \cdot -1 = 0 \,.$$

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 objects in our right pocket, then we write the coefficient as $\binom{7}{3,4}$. [Read as "7 *choose* 3-*comma*-4."] Evidently

$$\binom{N}{j} \underset{\text{with } k := N-j}{=\!=\!=} \binom{N}{j,\ k} \;=\; \frac{N!}{j!\,k!} \;=\; \frac{[\![N \downarrow j]\!]}{j!} \,.$$

Note $\binom{7}{0} = \binom{7}{0,7} = 1$. Also, $\binom{N+1}{k+1} = \binom{N}{k} + \binom{N}{k+1}$. Finally, the Binomial theorem says

$$B_1\text{:} \qquad [x+y]^N \;=\; \sum_{j+k=N} \binom{N}{j,k} \cdot x^j y^k \,,$$

where (j,k) ranges over all *ordered* pairs of natural numbers with sum N.

In general, for natnums $N = k_1 + \ldots + k_P$, the ***multinomial coefficient*** $\binom{N}{k_1,\, k_2,\, \ldots,\, k_P}$ is the number of ways of partitioning N objects, by putting k_1 objects in pocket-one, k_2 objects in pocket-two, ... putting k_P objects in the P^{th} pocket. Easily

$$B_2\text{:} \qquad \binom{N}{k_1, k_2, \ldots, k_P} \;=\; \frac{N!}{k_1! \cdot k_2! \cdot \ldots \cdot k_P!} \,.$$

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

$$B_1'\text{:} \qquad \binom{N}{k_1,\ldots,k_P} \cdot {x_1}^{k_1} \cdot {x_2}^{k_2} \cdots {x_P}^{k_P} \,,$$

taken over all natnum-tuples $\vec{k}$=$(k_1, \ldots, k_P)$ that sum to N.

§B Appendix

From `NumberTheory/mult-convolution^.latex`

There is little here that is not in the earlier pages, so I will eventually delete most of this.

Note: This appendix uses symbol $\precneqq$ to mean "*proper* divisor of".

Entrance. Fix a ring $\mathbf{R} = (\mathbf{R}, +, 0_{\mathbf{R}}, \cdot, 1_{\mathbf{R}})$ which is not necessarily commutative. Let $\mathbb{F}$ be the set of functions $\mathbb{Z}_+ \to \mathbf{R}$. Let $\mathbb{M} \subset \mathbb{F}$ be the subset of multiplicative functions. For $f, g \in \mathbb{F}$ define the ***convolution*** $f \circledast g \in \mathbb{F}$ by

$$[f \circledast g](n) := \sum_{d \bullet\!| n} f(d) g(\tfrac{n}{d}) \,.$$

Observe that

$$14: \qquad [f \circledast g](n) := \sum_{e \bullet\!| n} f(\tfrac{n}{e}) g(e) \,.$$

Definition. Let $\mathbb{M} \subset \mathbb{F}$ be the set of multiplicative functions, where f is ***multiplicative*** if:

$$k \perp n \implies f(k \cdot n) = f(k) f(n) \,.$$

Define functions $\zeta, \mathbf{1}, \delta \in \mathbb{M}$: ζ is the constant zero function, $\mathbf{1}$ is the constant one function, and $\delta(1) := 1_{\mathbf{R}}$ and $\delta(\neq 1) := 0_{\mathbf{R}}$. For every f, evidently,

$$[\delta \circledast f](n) = \sum_{d \bullet\!| n} \delta(d) f(n/d) = \delta(1) f(n/1) = f(n)$$

and similarly $[f \circledast \delta](n) = f(n)$. Thus δ is a two-sided identity for convolution. It is also evident that $\zeta \circledast f = \zeta = f \circledast \zeta$, so ζ is a zero-element for convolution.

15: Ring Theorem.

a: $\Omega := (\mathbb{F}, \circledast, \delta, +, \zeta)$ *is a ring.*

b: *Both* α *and* β *are ring-homomorphisms*

$$\beta : \Omega \twoheadrightarrow \mathbf{R} \qquad \alpha : \mathbf{R} \hookrightarrow \Omega$$
$$f \mapsto f(1) \qquad x \mapsto x\delta$$

so that $\beta \circ \alpha$ *is the identity map on* $\mathbf{R}$. *Consequently* Ω *is commutative IFF* $\mathbf{R}$ *is commutative.*

c: f *is a unit in* Ω *IFF* $f(1)$ *is a unit in* $\mathbf{R}$.

d: *If* f *is a zero-divisor in* Ω *then* $f(1)$ *is a zero-divisor in* $\mathbf{R}$. ♢

Pf of (a,b). Associativity of convolution follows from

$$\begin{aligned}
&[[f \circledast g] \circledast h](n) \\
&= \sum_{d \bullet\!| n} [f \circledast g](n/d) \cdot h(d) = \sum_{d \bullet\!| n} \sum_{e \bullet\!| \frac{n}{d}} f(e) g(\tfrac{n/d}{e}) h(d) \\
&= \sum_{d,e:\, d \cdot e \bullet\!| n} f(e) g(\tfrac{n}{d \cdot e}) h(d) = \sum_{e \bullet\!| n} f(e) \sum_{d \bullet\!| \frac{n}{e}} g(\tfrac{n/e}{d}) h(d) \\
&= \sum_{e \bullet\!| n} f(e) \cdot [g \circledast h](n/e) \overset{\text{def}}{=\!=} [f \circledast [g \circledast h]](n) \,.
\end{aligned}$$

Automatically, convolution distributes over addition,

$$\begin{aligned}
[f_1 + f_2] \circledast g &= f_1 \circledast g + f_2 \circledast g \quad \text{and} \\
f \circledast [g_1 + g_2] &= f \circledast g_1 + f \circledast g_2 \,,
\end{aligned}$$

since the multiplication in $\mathbf{R}$ distributes over addition.

Note that part (b) is a triviality. ♦

Pf of (c). We wish to define a $g \in \Omega$ so that $g \circledast f = \delta$. For each n, then, g must satisfy

$$\begin{aligned}
g(n) \cdot f(1) &\overset{\text{note}}{=\!=} g(n) \cdot f(\tfrac{n}{n}) \\
&= \delta(n) - \sum_{d : d \precneqq n} g(d) f(\tfrac{n}{d}) \,. \qquad 16:
\end{aligned}$$

Since $f(1)$ is by hypothesis an invertible element of $\mathbf{R}$, we can divide by $f(1)$ and express $g(n)$ in terms of $g(d)$ for smaller elements d. Since the $\precneqq$-order is well-founded, (16) gives a valid recursive definition of g. Note, by that way, that $g(1)$ will be $1/f(1)$.

A similar recursion constructs a function g' such that $f \circledast g' = \delta$. By associativity, then,

$$g = g \circledast [f \circledast g'] = [g \circledast f] \circledast g' = g' \,.$$ ♦

Proof of d. Suppose that there is a $g \neq \zeta$ such that $g \circledast f = \zeta$. Let n be $\bullet\!|$-smallest so that $g(n) \neq 0_{\mathbf{R}}$. Thus

$$\begin{aligned}
g(n) f(1) &= -\sum_{d \, d \precneqq n} g(d) f(\tfrac{n}{d}) \,. \\
&= -\sum_{d \, d \precneqq n} 0_{\mathbf{R}} \cdot f(\tfrac{n}{d}) = 0_{\mathbf{R}} \,.
\end{aligned}$$

Thus $f(1)$ is indeed a zero-divisor in $\mathbf{R}$. ♦
