

Multiplicative Functions: NumThy

Jonathan L.F. King
 University of Florida, Gainesville FL 32611-2082, USA
 squash@ufl.edu
 Webpage <http://squash.1gainesville.com/>
 14 August, 2018 (at 12:25)

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 $f, g: \mathbb{Z}_+ \rightarrow \mathbb{C}$, define their **convolution** (“Dirichlet convolution”) by

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

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 $f: \mathbb{Z}_+ \rightarrow \mathbb{C}$ 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 $k \mid n$ for “ k divides n ”. Its negation $k \nmid n$ means “ k does not divide n .” Use $n \bullet k$ and $n \nmid k$ 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 $n \parallel p^E$ 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 $K \nmid \Gamma$. This class is less important than \mathbb{M} . Indeed, the set of *totally* multiplicative fncs is not sealed under convolution.

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

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

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

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

$$\begin{aligned} \tau(n) &:= \sum_{d:d \mid n} 1 \quad \text{and} \\ \sigma(n) &:= \sum_{d:d \mid n} d. \quad \text{Generalizing} \\ \sigma_\alpha(n) &:= \sum_{d:d \mid n} d^\alpha, \quad \text{for } \alpha \in \mathbb{C}. \end{aligned}$$

This τ is called the **divisor-count** function, and σ is called the **divisor-sum** fnc. E.g., $\sigma(4) = 1 + 2 + 4 = 7$ and $\tau(4) = 1 + 1 + 1 = 3$. Note that $\sigma_0 = \tau$ and $\sigma_1 = \sigma$. Also...

1: *Each of $\delta, \mathbf{1}, \text{Id}, \tau, \sigma_\alpha$ is multiplicative.*

Exer 1: Use the uniqueness part of **FTArithmetic** to prove τ multiplicative. [Same argument applies to σ_α .]

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

$$\begin{aligned} 2a: \quad \tau(p^L) &= L + 1. \\ 2b: \quad \text{For } \alpha \neq 0: \quad \sigma_\alpha(p^L) &= \frac{p^{[L+1]\alpha} - 1}{p^\alpha - 1}. \end{aligned}$$

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.** *$(\widehat{\mathbb{G}}, \otimes, \delta)$ 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 $[f \circledast Id](K) = \sum_{a \cdot b = K} f(a) \cdot \delta(b) = f(K) \cdot \delta(1) \stackrel{\text{note}}{=} f(K)$.

(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

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

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

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

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,

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

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

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

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

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

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

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

since, by (3c), our h is multiplicative on all the (b, β) pairs on RhS(*). Adding $f(1 \cdot 1)h(K)h(\Gamma)$ to each side [again using that $f(1 \cdot 1) = 1$], 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

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

Putting it all together,

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

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

4: Lemma. Suppose that f and g are MFncs. Then $f \cdot g$ (pointwise product) is a MFnc. If g is no-where zero, then ptwise quotient f/g is a MFnc. **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 MFnc-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* μ to be the convolution-inverse of $\mathbf{1}$. I.e. $\boxed{\mu := \mathbf{1}^{\circledast -1}}$, so μ is characterized by $\mu \circledast \mathbf{1} = \delta$. By Thm 3, it is enough to know $\mu()$'s values on the powers of primes.

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

$$\mu(p) = -1 \quad \text{and} \quad \mu(p^n) = 0. \quad \diamond$$

Proof. Well $0 = \delta(p) = \mu(p) + \mu(1) = \mu(p) + 1$.

For a higher power of p :

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

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

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

$$\text{a: } [1..N] \hookrightarrow \bigsqcup_{d:d \mid N} \Phi(d) \times \{d\} \stackrel{\text{note}}{=} \left\{ (x, d) \mid \begin{array}{l} d \mid N \\ x \in \Phi(d) \end{array} \right\}$$

realized by the mapping

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

The inverse bijection is

$$\text{c: } (x, d) \mapsto x \cdot \frac{N}{d}. \quad \diamond$$

We now establish a few useful relations.

7: **Basic Lemma.** Among MFncs $\mathbf{1}, \tau, \sigma, \text{Id}, \mu$ and φ , the following relations hold.

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

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

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

iv: $\varphi \circledast \tau = \sigma$ and $\varphi \circledast \sigma = \text{Id}^{\circledast 2}$. \diamond

Proof of iii. Take cardinalities in (6a), which gives $\text{Id} = \varphi \circledast \mathbf{1}$. As for (iv), note that

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

which is σ , by definition. \diamond

7a: **Coro.** Euler φ is multiplicative. \diamond

Proof. Courtesy (7iii), $\varphi = \text{Id} \circledast \mathbf{1}$ is a convolution of MFncs, hence is an MFnc itself, by (3). \diamond

8: **Prop'n.** The fnc φ/Id is multiplicative. And

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

c: Finally, $\varphi(K) \rightarrow \infty$ as $K \nearrow \infty$. \diamond

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

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

Pf of (c). FTSOC, imagine a seq. $K_1 < K_2 < \dots$ along which $\varphi()$ 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 $L \leq 100$. Exer 4. Now...? \diamond

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

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

These are routinely proved by induction on n .

Applications of Möbius Inversion

An N^{th} -root ω of unity [in \mathbb{C}] 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

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

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

$$9b: \quad F_N(x) = \prod_{d \mid N} \mathbf{C}_d(x).$$

Used recursively, we compute these cyclo-polys:

$$9c: \quad \text{Examples:}$$

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

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 $\mu(N)$. Their product is 1, except when $N = 2$ where the product is -1. \diamond

Pf for all roots. Let S be the sum⁴, and P the product, of the set, \mathbf{A} , of all N^{th} -roots. Thus

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

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

$$\sum_{a \cdot b = N} \mathcal{S}(a) = [\text{Sum of all } N^{\text{th}} \text{ roots}] = \delta(N).$$

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

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 $N = 2$. \diamond

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

⁴For 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 $|\mathbf{V}_N| \stackrel{\text{note}}{=} \varphi(N)$. When $N \in [2.. \infty)$, moreover, \mathbf{C}_N is *palindromic* in that $\overleftarrow{\mathbf{C}_N} = \mathbf{C}_N$.

Finally, for $N \geq 2$ and $K := \varphi(N)$,

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

Proof. Equation (9b) gives

$$\mathbf{C}_N = F_N / \prod_{d \neq N} \mathbf{C}_d.$$

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

$$x \cdot [\frac{1}{x} - Z] = -1 \cdot [xZ - 1] = -1 \cdot Z \cdot [x - \frac{1}{Z}].$$

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

$$\prod_{Z \in \mathbf{V}_N} x \cdot [\frac{1}{x} - Z] = [-1]^K \cdot \left[\prod_{Z \in \mathbf{V}_N} Z \right] \cdot \prod_{Z \in \mathbf{V}_N} [x - \frac{1}{Z}].$$

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

$$\overleftarrow{\mathbf{C}_N}(x) = 1 \cdot 1 \cdot \prod_{Z \in \mathbf{V}_N} [x - \frac{1}{Z}] \stackrel{\text{note}}{=} \mathbf{C}_N(x).$$

Lastly, (11a) follows from (10). \diamond

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

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

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

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

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 $b \mid P^2$ means that a has form either αP^L or αP^K . So

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

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

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

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

$$\begin{aligned} \mathbf{C}_{NRR\Gamma}(z) &\xrightarrow{\text{by } (\dagger_N)} \prod_{a \cdot b = N} \mathbf{C}_{R\Gamma}(z^a)^{\mu(b)} \\ &\xrightarrow{\text{by } (\ddagger)} \prod_{a \cdot b = N} \left[\prod_{i \cdot j = R} \mathbf{C}_\Gamma([z^a]^i)^{\mu(j)} \right]^{\mu(b)} \\ &= \prod_{\substack{a \cdot b = N \\ i \cdot j = R}} \mathbf{C}_\Gamma(z^{ai})^{\mu(bj)}. \end{aligned}$$

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

$$\mathbf{C}_{M\Gamma}(z) = \prod_{x \cdot y = NR} \mathbf{C}_\Gamma(z^x)^{\mu(y)}. \quad \diamond$$

§A Appendix

A For a natnum n , use “ $n!$ ” to mean “ n *factorial*”; the product of all posints $\leq n$. 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

$$[\beta \downarrow j] := \beta \cdot [\beta - 1] \cdot [\beta - 2] \cdot \dots \cdot [\beta - [j-1]] ;$$

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

$$[\frac{2}{7} \downarrow 4] = \frac{2}{7} \cdot \frac{-5}{7} \cdot \frac{-12}{7} \cdot \frac{-19}{7} \text{ and } [1 \downarrow 3] = 1 \cdot 0 \cdot -1 = 0 .$$

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

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

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

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

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

In general, for natnums $N = k_1 + \dots + k_P$, the *multinomial coefficient* $\binom{N}{k_1, k_2, \dots, k_P}$ 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

$$B_2: \quad \binom{N}{k_1, k_2, \dots, k_P} = \frac{N!}{k_1! \cdot k_2! \cdot \dots \cdot k_P!} .$$

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

$$B'_1: \quad \binom{N}{k_1, \dots, k_P} \cdot x_1^{k_1} \cdot x_2^{k_2} \cdots x_P^{k_P} ,$$

taken over all natnum-tuples $\vec{k} = (k_1, \dots, k_P)$ 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 $\not\preceq$ 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 $\mathbb{Z}_+ \rightarrow \mathbf{R}$. 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

$$[f \circledast g](n) := \sum_{d \mid n} f(d)g\left(\frac{n}{d}\right).$$

Observe that

$$14: \quad [f \circledast g](n) := \sum_{e \mid n} f\left(\frac{n}{e}\right)g(e).$$

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,

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

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

$$\begin{array}{ll} \beta: \Omega \rightarrow \mathbf{R} & \alpha: \mathbf{R} \hookrightarrow \Omega \\ f \mapsto f(1) & x \mapsto x\delta \end{array}$$

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

$$\begin{aligned} [[f \circledast g] \circledast h](n) &= \sum_{d \mid n} [f \circledast g](n/d) \cdot h(d) = \sum_{d \mid n} \sum_{e \mid d} f(e)g\left(\frac{n}{de}\right)h(d) \\ &= \sum_{d, e: d \mid e \mid n} f(e)g\left(\frac{n}{d}\right)h(d) = \sum_{e \mid n} f(e) \sum_{d \mid \frac{n}{e}} g\left(\frac{n}{d}\right)h(d) \\ &= \sum_{e \mid n} f(e) \cdot [g \circledast h](n/e) \stackrel{\text{def}}{=} [f \circledast [g \circledast h]](n). \end{aligned}$$

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

$$\begin{aligned} 16: \quad g(n) \cdot f(1) &\stackrel{\text{note}}{=} g(n) \cdot f\left(\frac{n}{n}\right) \\ &= \delta(n) - \sum_{d: d \not\preceq n} g(d)f\left(\frac{n}{d}\right). \end{aligned}$$

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 $\not\preceq$ -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,

$$g = g \circledast [f \circledast g'] = [g \circledast f] \circledast g' = g'. \quad \color{red}{◆}$$

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

$$\begin{aligned} g(n)f(1) &= - \sum_{d: d \not\preceq n} g(d)f\left(\frac{n}{d}\right) \\ &= - \sum_{d: d \not\preceq n} 0_{\mathbf{R}} \cdot f\left(\frac{n}{d}\right) = 0_{\mathbf{R}}. \end{aligned}$$

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