Generating functions: Combinatorics

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
12 May, 2024 (at *13:15*)

ABSTRACT: Examples of generating-fnc use. As usual, we will ignore the issue of series convergence. The example by Derek Ledbetter uses the Möbius inversion formula.

Nomenclature. We use Wilf's notation from his book, GENERATINGFUNCTIONOLOGY.

Counting irreducible monic polynomials over a finite field

This is Derek Ledbetter's solution. Let $\Bbbk$ be a finite field; let $\mathsf{F} := |\Bbbk|$. Henceforth

1: *All "polys" (polynomials) have coefficients in $\Bbbk$ and are* <u>*monic*</u>.

[In particular, a "poly" is not Zip.] Let $\mathcal{A}_D$ denote the number of (All, monic) polys of degree–D. Thus

$$\mathcal{A}_D = \mathsf{F}^D, \qquad \text{for } D = 0, 1, 2 \ldots .$$

Each poly can be written uniquely as a product of irreducibles; the constant poly 1 is the empty product. For each $N \in \mathbb{Z}_+$, let $\mathcal{I}_N$ denote the number of *irreducible*[♡1] polys of deg–N. Hence $\mathcal{I}_1 = \mathsf{F}$ since, for each $\mathsf{c} \in \Bbbk$, the $x + \mathsf{c}$ polynomial is irreducible.

2: Theorem. *For each posint N, the number of irreducible degree–N monic polynomials is*

$$??': \qquad \mathcal{I}_N = \frac{1}{N} \sum_{k:\, k \bullet| N} \mathsf{F}^k \cdot \boldsymbol{\mu}(N/k)\,.$$

(Our convention for such sums is that the variable, here "k", ranges only over *positive* divisors.)

[♡1] In a commutative ring, my defn of ***irreducible*** is a non–zero-divisor, non-unit which only factors trivially. The only monic degree-zero poly is 1, which is a unit in this ring.

Remark. The $\boldsymbol{\mu}(\cdot)$ above is **the Möbius function**. (See `NumberTheory/multiplicative_fncs.latex` for more on this fnc.) The Möbius inversion formula says, for an arbitrary function $g{:}\mathbb{Z}_+ \to \mathbb{C}$, that the relation

$$h(k) := \sum_{N:\, N \bullet| k} g(N)\,, \quad \textit{can be inverted to}$$

$$g(N) = \sum_{k:\, k \bullet| N} h(k) \cdot \boldsymbol{\mu}(N/k)\,.$$

An application of (**??**) gives Fermat's Little Thm: Take $N = p$ prime. So $\mathcal{I}_p = \frac{1}{p}\big[\mathsf{F}^p - \mathsf{F}\big]$. But $\mathcal{I}_p$ is an integer, so F^p is mod-p congruent to F. □

Proof. Enumerate the irreducible deg-N polys as

$$q_{N,1} \quad q_{N,2} \quad \ldots \quad q_{N,i} \quad \ldots \quad q_{N,\mathcal{I}_N - 1} \quad q_{N,\mathcal{I}_N}\,.$$

Fix a poly $\mathbf{y}(\cdot)$, and use D for its degree. Let $Y_{N,i}$ count the number of times the factor $q_{N,i}$ occurs in the [unique] factorization of $\mathbf{y}$. Thus

$$3: \qquad \mathbf{y}(x) = \prod_{N=1}^{\infty} \prod_{i=1}^{\mathcal{I}_N} \Big[q_{N,i}(x)\Big]^{Y_{N,i}}\,,$$

where $Y_{N,i}$ is zero for all but finitely many (N, i) pairs. We can thus write the degree of $\mathbf{y}$ as

$$4: \qquad D = \prod_{N=1}^{\infty} \sum_{i=1}^{\mathcal{I}_N} N \cdot Y_{N,i}\,.$$

Consider the product

$$5: \qquad \prod_{N=1}^{\infty} \prod_{i=1}^{\mathcal{I}_N} \Big[\sum_{J=0}^{\infty} [x^N]^J\Big]\,.$$

For each pair N, i there is a sum –in big brackets– corresponding to it. To the poly $\mathbf{y}(x)$ above, associate a particular product of monomials in (**??**) by selecting from the $(N, i)^{th}$-sum the term $[x^N]^{Y_{N,i}}$; i.e, the J^{th} monomial, where $J = Y_{N,i}$. The product of the ∞-many monomials so obtained [all but finitely-many are "1"] evidently equals x^D.

We have constructed a bijection between all deg-D polys –rather, their factorizations (**??**)– and products of monomials in (**??**) whose product is x^D. Thus

$$6: \quad \sum_{D=0}^{\infty} \mathcal{A}_D \cdot x^D = \prod_{N=1}^{\infty} \Big[\sum_{J=0}^{\infty} [x^N]^J \Big]^{\mathcal{I}_N}.$$

Obtaining $\mathcal{A}_D$ in terms of $(\mathcal{I}_N)_{N=1}^{\infty}$. In RhS(**??**), the N^{th}-sum equals

$$1 \big/ [1 - x^N]^{\mathcal{I}_N}.$$

And, since $\mathcal{A}_D = \mathsf{F}^D$, the LhS equals $1/[1 - \mathsf{F}x]$. Taking reciprocals gives

$$1 - \mathsf{F}x = \prod_{N \geq 1} [1 - x^N]^{\mathcal{I}_N}.$$

Take log of both sides, using the expansion $\log(1-z) = -\sum_{k=1}^{\infty} \frac{1}{k} z^k$, to yield

$$\sum_{k=1}^{\infty} \frac{1}{k} \mathsf{F}^k x^k = \sum_{N \geq 1} \mathcal{I}_N \sum_{K=1}^{\infty} \frac{1}{K} x^{NK}.$$

Apply the "$x \cdot \frac{\mathrm{d}}{\mathrm{d}x}$" operator to remove the fractions:

$$\sum_{k=1}^{\infty} \mathsf{F}^k x^k = \sum_{N \geq 1} \sum_{K=1}^{\infty} \Big[\mathcal{I}_N \cdot N x^{NK} \Big].$$

Finally, equating coefficients of x^k yields

$$7: \quad \mathsf{F}^k = \sum_{N:\, N \bullet\!| k} N \cdot \mathcal{I}_N.$$

Applying Möbius inversion to (**??**) yields the (**??**) formula. ♦

Keating's proof of integrality

With α and β ranging over the posints, define

$$8: \quad [\![N, \mathsf{F}]\!] := \sum_{\alpha \cdot \beta = N} \boldsymbol{\mu}(\alpha) \cdot \mathsf{F}^{\beta}.$$

9: Thm. *For each posint N and integer F, we have that $[\![N, \mathsf{F}]\!] \;|\!\bullet\; N$.* ♢

Proof (Keating). For each N-clump $p^e \bullet\!\| N$, we need to show that

$$10: \quad [\![N, \mathsf{F}]\!] \;|\!\bullet\; p^e.$$

Case: $p \nmid \mathsf{F}$ Thus $p^e \perp \mathsf{F}$, so we can apply Dirichlet's Thm to conclude that there is a prime $r \in [\mathsf{F} + p^e \mathbb{Z}]$. Courtesy (**??′**),

$$[\![N, r]\!] \;|\!\bullet\; N \overset{\text{note}}{|\!\bullet} p^e.$$

But $\mathsf{F} \equiv_{p^e} r$ and $[\![N, \cdot]\!]$ is an intpoly, so $[\![N, \mathsf{F}]\!] \equiv_{p^e} [\![N, r]\!]$. Hence (**??**).

Case: $p \bullet\!| \mathsf{F}$ In order to establish (**??**), IST-Show, for each pair $\alpha \cdot \beta = N$, that

$$\Big[\boldsymbol{\mu}(\alpha) \neq 0 \Big] \implies \Big[\mathsf{F}^{\beta} \;|\!\bullet\; p^e \Big].$$

Now $\boldsymbol{\mu}(\alpha) \neq 0$ means $p^2 \nmid \alpha$, i.e $p^{e-1} \bullet\!| \beta$. So $\beta \geq p^{e-1}$, since β is positive. Thus

$$\mathsf{F}^{\beta} \;|\!\bullet\; p^{p^{e-1}} \;|\!\bullet\; p^e,$$

by (**??**$*$). ♦

11: Prop'n. *For each $p \in [2 \,..\, \infty)$ and posint e: $p^{e-1} \geq e$. Consequently*

$$*: \quad p^{p^{e-1}} \;|\!\bullet\; p^e.$$

Pf. Trivially, $p^{1-1} = 1 \geq 1$. Inducting on e, then,

$$p^e \;=\; p \cdot p^{e-1} \;\geq\; p \cdot e \;=\; 1 + [p-1]e\,,$$

since $e \geq 1$. Thus $p^e \geq 1 + e$, courtesy $p \geq 2$. ♦

Keating's proof of positivity

Below, for posreals x, let $\widehat{x}$ mean $\log(x)$.

Given a real T, define the ***discrete derivative***

$$[\mathbf{D}_T h](s) \;:=\; h(s+T) - h(s)\,.$$

For two reals T and V, their discrete deriv-ops, $\mathbf{D}_T$ and $\mathbf{D}_V$, commute with each other.

Defn. A fnc $h{:}\mathbb{R}\to\mathbb{R}$ is ***hyper-increasing*** (Keating) if: h is ∞-ly diff'able and

$\forall_{\text{posints}} n:$ $h^{(n)}$ is strictly-increasing. □

12: Verifying hyper-increasing. *Suppose h is hyper-increasing and $T > 0$. Then $g := \mathbf{D}_T(h)$ is hyper-increasing.* ◊

Proof. Note $g^{(n)}(s) \;=\; h^{(n)}(s+T) - h^{(n)}(s)$. ♦

13: Prop'. *Fix a real* $\mathsf{F}{>}1$. *Then* $h(s) := \mathsf{F}^{\mathsf{e}^s}$ *is hyper-increasing.* ◊

Proof. Temporarily, a "pospoly" $r()$ is a poly whose coeffs are posreals. ISTShow, for each n, that $h^{(n)}(s)$ has form $r(\mathsf{e}^s) \cdot \mathsf{F}^{\mathsf{e}^s}$. Diff'ing this gives

$$[r'(\mathsf{e}^s)\cdot\mathsf{e}^s]\mathsf{F}^{\mathsf{e}^s} \;+\; r(\mathsf{e}^s)\cdot[\mathsf{F}^{\mathsf{e}^s}\cdot\widehat{\mathsf{F}}\mathsf{e}^s] \;=\; \rho(\mathsf{e}^s)\cdot\mathsf{F}^{\mathsf{e}^s}\,,$$

where $\rho(\mathsf{e}^s)$ is $\left[r'(\mathsf{e}^s) + r(\mathsf{e}^s)\widehat{\mathsf{F}}\right]\cdot\mathsf{e}^s$. And this $\rho()$ is a pospoly, because $\mathsf{F} > 1$ and therefore $\widehat{\mathsf{F}} > 0$. ♦

14: Positivity Thm. *For each posreal* F *and posint N, expression $[\![N,\mathsf{F}]\!]$ from* (**??**) *is positive.* ◊

Pf. Write $N = P{\cdot}L$, where $P = \mathsf{p}_1\cdot\mathsf{p}_2\cdot\ldots\cdot\mathsf{p}_K$ is the product of the distinct primes in N. Since $\boldsymbol{\mu}(\alpha)$ is zero whenever some p^2 divides α, necessarily

$$[\![N,\mathsf{F}]\!] \;=\; \Big[\sum_{\alpha\cdot\beta=P}\boldsymbol{\mu}(\alpha)\,\mathsf{F}^{\beta L}\Big] \;\stackrel{\text{note}}{=\!=}\; [\![P,\mathsf{F}^L]\!]\,.$$

So WLOGenerality, N is square-free.

Write $N = \mathsf{p}_1\cdot\mathsf{p}_2\cdot\ldots\cdot\mathsf{p}_K$ as a product of distinct primes.

Whoa! Is this unfinished?
Filename: `Problems/Combinatorics/generating_func.latex`
As of: *Wednesday 22Feb2006.* Typeset: *12May2024 at 13:15.*