

Generating functions: Combinatorics

Jonathan L.F. King
 University of Florida, Gainesville FL 32611-2082, USA
 squash@ufl.edu
 Webpage <http://squash.1gainesville.com/>
 9 August, 2016 (at 21:18)

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 \mathbf{F} be a finite field; let $\mathcal{F} := \#\mathbf{F}$. Henceforth

1: All "polys" (polynomials) have coefficients in \mathbf{F} and are monic.

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

$$\mathcal{A}_D = \mathcal{F}^D, \quad \text{for } D = 0, 1, 2, \dots$$

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 $\mathcal{I}_1 = \mathcal{F}$ since, for each $c \in \mathbf{F}$, polynomial $x + c$ is irreducible.

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

$$2': \quad \mathcal{I}_N = \frac{1}{N} \sum_{k: k \bullet N} \mathcal{F}^k \cdot \mu(N/k). \quad \diamond$$

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

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

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

An application of (2') gives Fermat's Little Thm: Take $N = p$ prime. So $\mathcal{I}_p = \frac{1}{p} [\mathcal{F}^p - \mathcal{F}]$. But \mathcal{I}_p is an integer, so \mathcal{F}^p is mod- p congruent to \mathcal{F} . \square

Proof. Enumerate the irreducible deg- N polys as

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

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

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

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

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

Consider the product

$$5: \quad \prod_{N=1}^{\infty} \prod_{i=1}^{\mathcal{I}_N} \left[\sum_{J=0}^{\infty} [x^N]^J \right].$$

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 (5) 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 (3)– and products of monomials in (5) whose product is x^D . Thus

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

Obtaining \mathcal{A}_D in terms of $(\mathcal{I}_N)_{N=1}^{\infty}$. In RhS(6), the N^{th} -sum equals

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

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

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

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

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

Apply the “ $x \cdot \frac{d}{dx}$ ” operator to remove the fractions:

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

Finally, equating coefficients of x^k yields

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

Applying Möbius inversion to (7) yields the (2') formula. ♦

Keating's proof of integrality

With α and β ranging over the posints, define

$$8: \quad \llbracket N, \mathcal{F} \rrbracket := \sum_{\alpha \cdot \beta = N} \mu(\alpha) \cdot \mathcal{F}^{\beta}.$$

9: Thm. For each posint N and integer \mathcal{F} , we have that $\llbracket N, \mathcal{F} \rrbracket \bullet N$. ♦

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

$$10: \quad \llbracket N, \mathcal{F} \rrbracket \bullet p^e.$$

CASE: $p \nmid \mathcal{F}$ Thus $p^e \perp \mathcal{F}$, so we can apply Dirichlet's Thm to conclude that there is a prime $r \in \mathcal{F} + p^e \mathbb{Z}$. Courtesy (2'),

$$\llbracket N, r \rrbracket \bullet N \overset{\text{note}}{\bullet} p^e.$$

But $\mathcal{F} \equiv_{p^e} r$ and $\llbracket N, \cdot \rrbracket$ is an intpoly, so $\llbracket N, \mathcal{F} \rrbracket \equiv_{p^e} \llbracket N, r \rrbracket$. Hence (10).

CASE: $p \mid \mathcal{F}$ In order to establish (10), IST-Show, for each pair $\alpha \cdot \beta = N$, that

$$[\mu(\alpha) \neq 0] \implies [\mathcal{F}^{\beta} \bullet p^e].$$

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

$$\mathcal{F}^{\beta} \bullet p^{p^{e-1}} \bullet p^e,$$

by (11*). ♦

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

$$*: \quad p^{p^{e-1}} \bullet p^e. \quad \diamond$$

Proof. Well $p^{1-1} = 1 \geq 1$. Inducting on e , then, $p^e = p \cdot p^{e-1} \geq p \cdot e = 1 + [p-1]e$, since $e \geq 1$. Thus $p^e \geq 1 + e$, since $p \geq 2$. ♦

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 $h: \mathbb{R} \rightarrow \mathbb{R}$ is **hyper-increasing** (Keating) if: h is ∞ -ly diff'able and $\forall_{\text{posints } n} : h^{(n)}$ is strictly-increasing. \square

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

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

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

Proof. Temporarily, a "pospoly" $r()$ is a poly whose coeffs are posreals. ISTShow, for each n , that $h^{(n)}(s)$ has form $r(e^s) \cdot \mathcal{F}^{e^s}$. Diff'ing this gives $[r'(e^s) \cdot e^s] \mathcal{F}^{e^s} + r(e^s) \cdot [\mathcal{F}^{e^s} \cdot \widehat{\mathcal{F}} e^s] = \rho(e^s) \cdot \mathcal{F}^{e^s}$, where $\rho(e^s)$ is $[r'(e^s) + r(e^s) \widehat{\mathcal{F}}] \cdot e^s$. And this $\rho()$ is a pospoly, because $\mathcal{F} > 1$ and therefore $\widehat{\mathcal{F}} > 0$. \diamond

14: Positivity Thm. For each posreal \mathcal{F} and posint N , expression $[[N, \mathcal{F}]]$ from (8) is positive. \diamond

Proof. First write $N = P \cdot L$, where $P = p_1 \cdot p_2 \cdot \dots \cdot p_K$ is the product of the distinct primes in N . Since $\mu(\alpha)$ is zero whenever some p^2 divides α , necessarily

$$[[N, \mathcal{F}]] = \left[\sum_{\alpha \cdot \beta = P} \mu(\alpha) \mathcal{F}^{\beta L} \right] \stackrel{\text{note}}{=} [[P, \mathcal{F}^L]]. \quad \diamond$$

So $\overline{\text{WLOGenerality, } N \text{ is square-free}}$.

Write $N = p_1 \cdot p_2 \cdot \dots \cdot p_K$ as a product of distinct primes.

Filename: Problems/Combinatorics/generating_func.latex
As of: Wednesday 22Feb2006. Typeset: 9Aug2016 at 21:18.