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

1: All “polys” (polynomials) have coefficients in $F$ 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

$$\mathcal{A}_D = \mathcal{F}^D,$$

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\(^\dagger\) polys of deg-$N$. Hence $\mathcal{I}_1 = \mathcal{F}$ since, for each $c \in F$, polynomial $x + c$ is irreducible.

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

$$\mathcal{I}_N = \frac{1}{N} \sum_{k} \mathcal{F}^k \cdot \mu(N/k).$$

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

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 $g: \mathbb{Z}_+ \to \mathbb{C}$, that the relation

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

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

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

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 $y(\cdot)$, 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 $y$. Thus

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

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

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

Consider the product

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

For each pair $N,i$ there is a sum—in big brackets—corresponding to it. To the poly $y(x)$ above, associate a particular product of monomials in (5) by selecting from the $(N,i)$’th sum the term $[x^J]^{Y_{N,i}}$, i.e, the $J$’th monomial, where $J = Y_{N,i}$. The product of the $\infty$-many monomials so obtained (all but finitely-many are “1”) evidently equals $x^D$.

\(\oplus\)=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.
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

$$
6: \sum_{D=0}^{\infty} A_D \cdot x^D = \prod_{N=1}^{\infty} \left[ \sum_{J=0}^{\infty} [x^N]^J \right]^{I_N}.
$$

**Obtaining $A_D$ in terms of $(I_N)_{N=1}^{\infty}$.** In RhS(6), the $N^{th}$-sum equals

$$
1/[1 - x^N]^{I_N}.
$$

And, since $A_D = F^D$, the LhS equals $1/[1 - Fx]$. Taking reciprocals gives

$$
1 - Fx = \prod_{N \geq 1} [1 - x^N]^{I_N}.
$$

Take log of both sides, using the expansion

$$
\log(1 + y) = -\sum_{k=1}^{\infty} \frac{1}{k} y^k,
$$

to yield

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

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

$$
\sum_{k=1}^{\infty} F^k x^k = \sum_{N \geq 1} \sum_{K=1}^{\infty} I_N \cdot N x^{NK}.
$$

Finally, equating coefficients of $x^k$ yields

$$
7: \quad F^k = \sum_{N: N \cdot k} N \cdot I_N.
$$

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

**Keating’s proof of integrality**

With $\alpha$ and $\beta$ ranging over the posints, define

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

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

$$
10: \quad [N, F] \perp p^e.
$$

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

$$
[N, r] \perp N \quad \text{note} \quad p^e.
$$

But $F ≡ r \mod N$, so $[N, F] ≡ p^e \mod [N, r]$. Hence (10).

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

$$
[N, F] \perp p^e.
$$

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

$$
[F^\beta] \perp p^{e-1} \perp p^e;
$$

by (11∗).

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

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

**Proof.** Well $p^{e-1} = 1 \geq 1$. Inducting on $e$, then,

$$
p^e = p \cdot p^{e-1} \geq p \cdot e = 1 + [p-1]e, \quad \text{since } e \geq 1.
$$

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

**Keating’s proof of positivity**

Below, for posreals $x$, let $\left\lfloor \hat{x} \right\rfloor$ mean $\log(x)$.

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

$$
[D_T h](s) := h(s + T) - h(s).
$$

For two reals $T$ and $V$, their discrete deriv-ops, $D_T$ and $D_V$, commute with each other.
Defn. A func \( h: \mathbb{R} \to \mathbb{R} \) is **hyper-increasing** (Keating) if: \( h \) is \( \infty \)-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 \( g := D_T(h) \) is hyper-increasing.

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

13: Prop’. Fix a real \( F > 1 \). Then \( h(s) := F^e_s \) 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 \( r(e^s) \cdot F^{e^s} \). Diff’ing this gives

\[
[r'(e^s) \cdot e^s]F^{e^s} + r(e^s) \cdot [F^{e^s} \cdot \hat{F} e^s] = \rho(e^s) \cdot F^{e^s},
\]

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

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

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

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

So \( \text{WLOGenality, } N \) is square-free.

Write \( N = p_1 \cdot p_2 \cdot \ldots \cdot p_K \) as a product of distinct primes.