A TALE OF TWO CYCLICITIES: COUNTING IN FINITE CYCLIC GROUPS AND FINITE FIELDS

JONATHAN COHEN AND ALAN ROCHE

Abstract. We study several combinatorial identities that arise naturally from the structure of finite cyclic groups and finite extensions of finite fields. We are particularly interested in interconnections between the identities.

Introduction.

We use standard facts about finite cyclic groups and finite fields to study several well-known combinatorial identities. The novelty of our article stems from our route to the identities and our focus on the close links between them.

To convey a sense of our approach, recall that a cyclic group $C = C_n$ of order n has $\phi(n)$ generators where ϕ is Euler's function. An element of C is a generator if and only if it does not belong to a maximal (proper) subgroup. Moreover, the maximal subgroups are precisely the subgroups of prime index, one for each prime divisor of n. The subgroup structure of C then leads, via some simple counting, to a well-known formula for $\phi(n)$. For example, in the case $n = 12$, there are exactly two maximal subgroups, one of index 2 and one of index 3, whose intersection is of index 6. It follows that

$$\phi(12) = 12 - \frac{12}{2} - \frac{12}{3} + \frac{12}{6}. \tag{i}$$

Now consider a parallel cyclic structure: for q a prime power, look at the degree n extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of finite fields. How many generators does it have, that is, how many elements $\alpha \in \mathbb{F}_{q^n}$ satisfy $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$? Observe that α generates $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if α does not belong to a maximal (proper) subfield of $\mathbb{F}_{q^n}$ containing $\mathbb{F}_q$. These are precisely the subfields $\mathbb{F}_{q^{n/l}}$ as l varies through the prime divisors of n. Again some simple counting leads to a formula for the number of generators $\Psi_n(q)$ of $\mathbb{F}_{q^n}/\mathbb{F}_q$. For $n = 12$, it says

$$\Psi_{12}(q) = q^{12} - q^{12/2} - q^{12/3} + q^{12/6}. \tag{ii}$$

We write $N_n(q)$ for the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$. By some elementary field theory, which we review in Section 3, $\Psi_n(q) = nN_n(q)$. Thus the formula for $\Psi_n(q)$ also gives an expression for $N_n(q)$. This goes back to Gauss (for q prime) and is sometimes called Gauss's formula.

What explains the correspondence between (i) and (ii)? Formula (i) reflects the structure of the lattice of subgroups of C_n; formula (ii) arises in the same way from the lattice of intermediate fields of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ (for $n = 12$ in each case). By Galois theory, or

more elementary means, these lattices are really the same: each is isomorphic to the lattice of positive divisors of n.

We also look at five similar identities, so seven in all. The initial proofs, as in the sketch above, are via pleasant counting arguments (at least to our minds) that exploit the subgroup structure of C_n or the parallel structure of $\mathbb{F}_{q^n}/\mathbb{F}_q$. The identities can be transferred to certain convolution rings of functions. Using this interpretation, we show that they are formally equivalent—any one implies any other.

Much of what we say has been noted elsewhere. For example, we see that our use of counting to arrive at a polynomial expression for $\Psi_n(q)$, hence also Gauss's formula, appears in [7] (see Theorem 21.11) and [2]—and surely elsewhere. A similar argument is outlined as an exercise in [3] (see Exercise 14 in Section 11.2). There is an overlap too with parts of [1] and [8] and undoubtedly with many other references. There is no new thing under the sun in such well-traveled parts of the mathematical landscape. However, there is something new, we believe, in our overall perspective, particularly our focus on connections between the various formulæ.

Notation and Preliminaries.

For integers d and n, we write $d \mid n$ to indicate that d divides n. We only ever consider positive divisors of positive integers, so *divisor* for us always means *positive divisor*.

For integers a and b, we write (a, b) for the greatest common divisor of a and b. As usual, we say that a and b are *relatively prime* or that a is *relatively prime* to b if $(a, b) = 1$.

Euler's function ϕ has the lead role in our tale. For n a positive integer, recall that $\phi(n)$ counts the number of integers between 1 and n that are relatively prime to n, that is,

$$\phi(n) \;=\; \#\text{ integers } a \text{ with } 1 \le a \le n \text{ such that } (a, n) = 1.$$

The Möbius function μ also plays a prominent role. For m a positive integer,

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1, \\ (-1)^k & \text{if } m \text{ is a product of } k \text{ distinct primes}, \\ 0 & \text{otherwise.} \end{cases}$$

For example, $\mu(2) = \mu(3) = -1, \mu(4) = 0$, $\mu(6) = \mu(2 \cdot 3) = 1$. In supporting roles, we have the functions τ and σ. For n a positive integer,

$$\tau(n) \;=\; \#\text{ divisors of } n \;=\; \sum_{d|n} 1,$$

$$\sigma(n) \;=\; \text{sum of divisors of } n \;=\; \sum_{d|n} d.$$

We appeal twice to the inclusion-exclusion principle. For convenience, we recall the statement.

Inclusion-Exclusion Principle. *For finite sets* $A_1, \ldots, A_r$,

$$\left|\bigcup_{i=1}^{r} A_i\right| = \sum_i |A_i| - \sum_{j<k} |A_i \cap A_k| + \cdots + (-1)^{r-1}|A_1 \cap \cdots \cap A_r|.$$

We write $\mathbb{Z}$ for the set of integers. For us, $\mathbb{N} = \{1, 2, 3, \ldots\}$.

1. Counting with Finite Cyclic Groups.

Let n be a positive integer and $C = C_n$ be a cyclic group of order n. The subgroup structure of C is especially simple: C has a unique cyclic subgroup of order d for each d dividing n and no other subgroups. It follows that the lattice of subgroups of C is just the lattice of divisors of n. In particular, for any subgroups D_1 and D_2 of C,

$$|D_1 \cap D_2| = (|D_1|, |D_2|). \tag{a}$$

We use the subgroup structure of C to derive three well-known number-theoretic identities.

1.1. **First identity.** The group C has $\phi(n)$ generators. For $x \in C$,

$$\begin{aligned} x \text{ generates } C &\iff \langle x \rangle \text{ is not a proper subgroup of } C \\ &\iff x \text{ does not belong to a maximal (proper) subgroup of } C. \end{aligned}$$

The maximal subgroups of C are precisely the subgroups of prime index. Write $p_1, \ldots, p_r$ for the distinct prime divisors of n and C^i for the unique subgroup of C of index p_i, or order n/p_i, for $i = 1, \ldots, r$. Thus

$$\phi(n) = n - \left|\bigcup_{i=1}^{r} C^i\right|.$$

Hence, by the inclusion-exclusion principle and repeated use of (a),

$$\begin{aligned} \phi(n) &= n - \sum_i |C^i| + \sum_{j<k} |C^j \cap C^k| - \cdots + (-1)^r |C^1 \cap \cdots \cap C^r| \\ &= n - \sum_i \frac{n}{p_i} + \sum_{j<k} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} \qquad \text{(b)} \\ &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right). \qquad \text{(c)} \end{aligned}$$

Using the Möbius function, we can write (b) more compactly as

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}. \tag{1}$$

1.2. **Second identity.** Next we count the elements of C according to their orders. The argument is a staple of introductory abstract algebra courses. Each element of C has order d for some divisor d of n. Further, for a given divisor d, the elements of order d are precisely the $\phi(d)$ generators of the unique cyclic subgroup of C of order d. Thus

$$n = \sum_{d|n} \phi(d). \tag{2}$$

1.3. **Third identity.** Now consider

$$\Omega = \{(x, D) : D \leq C \text{ and } x \in D\}.$$

We count the number of elements in Ω in two ways by summing over the fibers of the two projections:

$$\begin{array}{ccccc} (x,D) & \longmapsto & D:\Omega & \longrightarrow & \{\text{subgroups of } C\} \\ \downarrow & & \downarrow & & \\ x & & C. & & \end{array}$$

This gives

$$\sum_{D \leq C} |\{x \in C : x \in D\}| \;=\; \sum_{x \in C} |\{D \leq C : x \in D\}|. \tag{▲}$$

Since C has a unique subgroup of order d for each divisor d of n and no other subgroups, the first sum is

$$\sum_{D \leq C} |D| \;=\; \sum_{d|n} d \;=\; \sigma(n).$$

For the second sum, note that for $x \in C$ and $D \leq C$,

$$\begin{aligned} x \in D &\iff \langle x \rangle \leq D \\ &\iff D/\langle x \rangle \leq C/\langle x \rangle. \end{aligned}$$

If x has order d then $C/\langle x \rangle$ is cyclic of order $\dfrac{n}{d}$ and so has $\tau\left(\dfrac{n}{d}\right)$ subgroups. Hence

$$\sum_{x \in C} |\{D \leq C : x \in D\}| \;=\; \sum_{d|n} \phi(d)\tau\left(\frac{n}{d}\right).$$

Thus (▲) says

$$\sigma(n) \;=\; \sum_{d|n} \phi(d)\tau\left(\frac{n}{d}\right). \tag{3}$$

2. Convolution Identities.

The identities (1)–(3) are equivalent—any one implies any other. There's an elegant way to see this via the following ring-theoretic construction.

Let $\mathcal{C}$ denote the set of functions $f : \mathbb{N} \to \mathbb{Z}$. Define addition and multiplication of elements $f, g \in \mathcal{C}$ by

$$\begin{aligned} (f+g)(n) &= f(n) + g(n), \\ (f \star g)(n) &= \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right), \qquad n \in \mathbb{N}. \end{aligned}$$

It's routine to check that $+$ and $\star$ make $\mathcal{C}$ into a commutative ring with identity. The (multiplicative) identity element is δ where

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Multiplication in $\mathcal{C}$ is often called the Dirichlet product or convolution.

Remark. We introduce only what we need to obtain equivalence of (1)–(3). See [1] for a more detailed and very pleasant discussion of the ring $\mathcal{C}$ and certain relatives, particularly their groups of units. The discussion continues in [4].

Define $\mathsf{1}, \mathsf{i} \in \mathcal{C}$ by

$$\begin{aligned} \mathsf{1}(n) &= 1, \\ \mathsf{i}(n) &= n, \qquad n \in \mathbb{N}. \end{aligned}$$

We can then rewrite (1)–(3) as identities in $\mathcal{C}$:

$$\phi = \mu \star \mathsf{i}, \tag{$1_\star$}$$

$$\mathsf{i} = \phi \star \mathsf{1}, \tag{$2_\star$}$$

$$\sigma = \phi \star \tau. \tag{$3_\star$}$$

Proposition. *The identities* $(1_\star), (2_\star), (3_\star)$ *are equivalent.*

To prove the proposition and for later use, we record a fundamental observation:

$$\mu \star \mathsf{1} = \delta. \tag{$1^\times$}$$

We'll also use a slight variant in another section:

$$(\mathsf{i}\mu) \star \mathsf{i} = \delta \tag{$2^\times$}$$

where $\mathsf{i}\mu$ is the pointwise product of i and μ, that is,

$$(\mathsf{i}\mu)(n) = n\mu(n), \qquad n \in \mathbb{N}.$$

Using $\mu(1) = 1 = \delta(1)$, we have

$$(\mu \star \mathsf{1})(1) = 1 = \delta(1),$$

so $(1^\times)$ holds for $n = 1$. In the same way, $(2^\times)$ holds for $n = 1$. Now let $n > 1$. Then

$$(\mu \star \mathsf{1})(n) = \sum_{d|n} \mu(d)$$

and

$$\begin{aligned} ((\mathsf{i}\mu) \star \mathsf{i})(n) &= \sum_{d|n} d\mu(d)\, \frac{n}{d} \\ &= n \sum_{d|n} \mu(d). \end{aligned}$$

Thus to establish $(1^\times)$ and $(2^\times)$, we have to show that

$$\sum_{d|n} \mu(d) = 0.$$

To this end, we again write $p_1, \ldots, p_r$ for the distinct prime divisors of n, so that

$$\begin{aligned}\sum_{d|n} \mu(d) &= 1 + \sum_i \mu(p_i) + \sum_{j<k} \mu(p_j p_k) + \cdots + \mu(p_1 \cdots p_r) \\ &= 1 - \binom{r}{1} + \binom{r}{2} - \cdots + (-1)^r \\ &= (1-1)^r \\ &= 0,\end{aligned}$$

as required. In other words, the functions μ, $\mathsf{1}$, i, $\mathsf{i}\mu$ belong to the group of units $\mathcal{C}^\times$ of $\mathcal{C}$ and $\mu^{-1} = \mathsf{1}$, $\mathsf{i}^{-1} = \mathsf{i}\mu$.

Proof of Proposition. Recall we want to prove equivalence of the formulæ

$$\phi = \mu \star \mathsf{i}, \tag{$1_\star$}$$

$$\mathsf{i} = \phi \star \mathsf{1}, \tag{$2_\star$}$$

$$\sigma = \phi \star \tau. \tag{$3_\star$}$$

We'll show that $(1_\star) \Leftrightarrow (2_\star) \Leftrightarrow (3_\star)$.

$(1_\star) \Leftrightarrow (2_\star)$: We rewrite $\phi = \mu \star \mathsf{i}$ as $\phi \star \mu^{-1} = \mathsf{i}$. By $(1^\times)$, $\mu^{-1} = \mathsf{1}$, so $(1_\star)$ and $(2_\star)$ are equivalent.

$(2_\star) \Leftrightarrow (3_\star)$: We have $\mathsf{i} = \phi \star \mathsf{1}$ if and only if $\mathsf{i} \star \mathsf{1} = \phi \star \mathsf{1} \star \mathsf{1}$. Now $\sigma = \mathsf{i} \star \mathsf{1}$ and $\tau = \mathsf{1} \star \mathsf{1}$, so $\mathsf{i} \star \mathsf{1} = \phi \star \mathsf{1} \star \mathsf{1}$ says exactly that $\sigma = \phi \star \tau$. □

3. Counting in Finite Fields.

We recall some standard facts about finite fields with a few words of justification. For more detail, see for example [5, Section 14.3] or the more elementary treatment in [6, Sections 7.1–7.2]. We'll use these facts to obtain q-versions of the identities (1)–(3).

Let q be a prime power. A field has q elements if and only if it is a splitting field over its prime field of the polynomial $\mathrm{X}^q - \mathrm{X}$. In this case, each element of the field is a root of $\mathrm{X}^q - \mathrm{X}$. In particular, the polynomial has no repeated roots. By uniqueness of splitting fields (up to isomorphism), there is a unique field of order q (up to isomorphism). We write $\mathbb{F}_q$ for any such field and refer to it, following standard practice, as *the* finite field of order q.

Now let n be a positive integer. Then $q-1 \mid q^n - 1$ and hence $\mathrm{X}^{q-1} - 1$ divides $\mathrm{X}^{q^n-1} - 1$ in $\mathbb{F}_q[\mathrm{X}]$, or equivalently $\mathrm{X}^q - \mathrm{X}$ divides $\mathrm{X}^{q^n} - \mathrm{X}$ in $\mathbb{F}_q[\mathrm{X}]$. Thus the field $\mathbb{F}_{q^n}$ contains a unique copy of $\mathbb{F}_q$. The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is closely related to the cyclic group C_n with n elements. The fundamental fact for our purposes is that the lattice of intermediate fields of $\mathbb{F}_{q^n}/\mathbb{F}_q$ is exactly the lattice of divisors of n. That is:

1) for each divisor d of n, there is a unique copy of $\mathbb{F}_{q^d}$ between $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ and the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ admits no other intermediate fields;
2) for any divisors d and d' of n, $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^{d'}}$ if and only if $d \mid d'$.

As a consequence of statement 2), we have the following analogue of the relation (a) in Section 1: for any divisors d and e of n,

$$\mathbb{F}_{q^d} \cap \mathbb{F}_{q^e} \;=\; \mathbb{F}_{q^{(d,e)}}. \tag{a$_q$}$$

We recall also that the automorphism group $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic of order n. More precisely, $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ admits a canonical generator of order n, the Frobenius automorphism Φ given by $\Phi(\lambda) = \lambda^q$, $\lambda \in \mathbb{F}_{q^n}$. Since the lattice of subgroups of C_n is just the lattice of divisors of n, statements 1) and 2) follow from the fundamental theorem of Galois theory. They can also be derived by elementary means from the characterizations of $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ as splitting fields.

For $\alpha \in \mathbb{F}_{q^n}$, we write $\min_{\mathbb{F}_q}\alpha$ for the minimal polynomial of α over $\mathbb{F}_q$, that is, the unique monic polynomial $f(\mathrm{X}) \in \mathbb{F}_q[\mathrm{X}]$ of least degree such that $f(\alpha) = 0$. Then $\min_{\mathbb{F}_q}\alpha$ is irreducible in $\mathbb{F}_q[\mathrm{X}]$ and $g(\alpha) = 0$ for $g(\mathrm{X}) \in \mathbb{F}_q[\mathrm{X}]$ if and only if $\min_{\mathbb{F}_q}\alpha$ divides $g(\mathrm{X})$.

We say that α *generates* $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$. For any $\alpha \in \mathbb{F}_{q^n}$,

$$[\mathbb{F}_q(\alpha) : \mathbb{F}_q] \;=\; \deg \min\nolimits_{\mathbb{F}_q}\alpha.$$

Thus α generates $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $\deg \min_{\mathbb{F}_q}\alpha = n$.

Suppose now that $f(\mathrm{X}) \in \mathbb{F}_q[\mathrm{X}]$ is monic and irreducible of degree n. Let α be a root of $f(\mathrm{X})$ in some extension of $\mathbb{F}_q$, so that $f = \min_{\mathbb{F}_q}\alpha$ and $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$. Thus $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$, so α is a root of $\mathrm{X}^{q^n} - \mathrm{X}$. It follows that $f(\mathrm{X})$ divides $\mathrm{X}^{q^n} - \mathrm{X}$ in $\mathbb{F}_q[\mathrm{X}]$. As $\mathrm{X}^{q^n} - \mathrm{X}$ has no repeated roots, we see that $f(\mathrm{X})$ has n distinct roots in $\mathbb{F}_{q^n}$.

To sum up, α generates $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if α is a root of a monic irreducible polynomial of degree n in $\mathbb{F}_q[\mathrm{X}]$. Moreover:

- each monic irreducible polynomial in $\mathbb{F}_q[\mathrm{X}]$ of degree n has n distinct roots in $\mathbb{F}_{q^n}$;
- if two monic irreducible polynomials over $\mathbb{F}_q$ share a root, say α, then they are equal—each must be $\min_{\mathbb{F}_q}\alpha$.

As in the introduction, we write $\Psi_n(q)$ for the number of generators of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $N_n(q)$ for the number of monic irreducible polynomials of degree n in $\mathbb{F}_q[\mathrm{X}]$. From our discussion, $\Psi_n(q) = nN_n(q)$.

We now begin to work toward suitable q-versions of the identities (1)–(3). The quantity $\Psi_n(q)$ will play the role of $\phi(n)$.

3.1. **First q-identity.** Note that

$$\begin{aligned} \alpha \text{ generates } \mathbb{F}_{q^n}/\mathbb{F}_q &\iff \mathbb{F}_q(\alpha) \text{ is not a proper subfield of } \mathbb{F}_{q^n} \\ &\iff \mathbb{F}_q(\alpha) \text{ is not contained in a maximal} \\ &\qquad \text{(proper) subfield of } \mathbb{F}_{q^n}. \end{aligned}$$

Write $l_1, \ldots, l_r$ for the distinct prime divisors of n. Then the maximal subfields of $\mathbb{F}_{q^n}/\mathbb{F}_q$ are the fields $\mathbb{F}_{q^{n/l_i}}$ for $i = 1, \ldots, r$. Thus

$$\Psi_n(q) \;=\; q^n - \left| \bigcup_{i=1}^{r} \mathbb{F}_{q^{n/l_i}} \right|.$$

Hence, by the inclusion-exclusion principle and repeated use of (a_q),

$$\begin{aligned}\Psi_n(q) &= q^n - \sum_i |\mathbb{F}_{q^{n/l_i}}| + \sum_{j<k} |\mathbb{F}_{q^{n/l_j}} \cap \mathbb{F}_{q^{n/l_k}}| - \cdots \\ &\qquad + (-1)^r |\mathbb{F}_{q^{n/l_1}} \cap \cdots \cap \mathbb{F}_{q^{n/l_r}}| \\ &= q^n - \sum_i q^{n/l_i} + \sum_{j<k} q^{n/l_j l_k} - \cdots + (-1)^r q^{n/l_1 \cdots l_r}.\end{aligned}$$

In more compact form,

$$\Psi_n(q) = \sum_{d|n} \mu(d) q^{n/d}. \tag{1_q}$$

3.2. **Second q-identity.** It's convenient to introduce the following terminology.

Definition. We say that $\alpha \in \mathbb{F}_{q^n}$ has *level* d if $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$. Equivalently, the level of α is the degree of $\min_{\mathbb{F}_q} \alpha$. For this reason, the level of α is sometimes called its degree.

We count the elements of $\mathbb{F}_{q^n}$ according to their levels. The level of each $\alpha \in \mathbb{F}_{q^n}$ is a divisor of n. Further, for a given divisor d, there are $\Psi_d(q)$ elements of level d. Hence

$$q^n = \sum_{d|n} \Psi_d(q). \tag{2_q}$$

3.3. **Third q-identity.** Next we consider the q-analogue Ω_q of the set Ω from Section 1. It consists of all pairs $(\alpha, \mathbb{E})$ where $\mathbb{E}$ is a subfield of $\mathbb{F}_{q^n}$ containing $\mathbb{F}_q$ and $\alpha \in \mathbb{E}$:

$$\Omega_q = \{(\alpha, \mathbb{E}) : \mathbb{F}_q \subseteq \mathbb{E} \subseteq \mathbb{F}_{q^n}, \mathbb{E} \text{ a field}, \alpha \in \mathbb{E}\}.$$

Again, we count $|\Omega_q|$ in two ways by summing over the fibers of the two projections:

$$\begin{array}{ccccc} (\alpha, \mathbb{E}) & \longmapsto & \mathbb{E} : \Omega_q & \longrightarrow & \{\text{subfields of } \mathbb{F}_{q^n} \text{ containing } \mathbb{F}_q\} \\ \downarrow & & \downarrow & & \\ \alpha & & \mathbb{F}_{q^n}. & & \end{array}$$

This gives

$$\sum_{\mathbb{F}_q \subseteq \mathbb{E} \subseteq \mathbb{F}_{q^n}} |\{\alpha \in \mathbb{F}_{q^n} : \alpha \in \mathbb{E}\}| = \sum_{\alpha \in \mathbb{F}_{q^n}} |\{\mathbb{E} \subseteq \mathbb{F}_{q^n} : \mathbb{F}_q(\alpha) \subseteq \mathbb{E}\}|. \tag{▼}$$

To not clutter the notation, we've left implicit the requirement that $\mathbb{E}$ is a field. We follow this convention for the remainder of the subsection.

Since $\mathbb{F}_{q^n}/\mathbb{F}_q$ has a unique intermediate field of order q^d for each divisor d of n and no other intermediate fields, the first sum is

$$\sum_{\mathbb{F}_q \subseteq \mathbb{E} \subseteq \mathbb{F}_{q^n}} |\mathbb{E}| = \sum_{d|n} q^d.$$

For the second sum, note that for $\alpha \in \mathbb{F}_{q^n}$, there is a unique divisor d of n such that $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$ (namely, the level of α). Then

$$\begin{aligned}\mathbb{F}_q(\alpha) \subseteq \mathbb{E} \subseteq \mathbb{F}_{q^n} &\iff \mathbb{F}_{q^d} \subseteq \mathbb{E} \subseteq \mathbb{F}_{q^n} \\ &\iff |\mathbb{E}| = q^{de} \text{ where } e \mid \frac{n}{d}.\end{aligned}$$

In other words, for a given α of level d, there are $\tau\left(\frac{n}{d}\right)$ choices for $\mathbb{E}$. Since there are $\Psi_d(q)$ elements of level d in $\mathbb{F}_{q^n}$,

$$\sum_{\alpha\in\mathbb{F}_{q^n}} |\{\mathbb{E}\subseteq\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)\subseteq\mathbb{E}\}| \;=\; \sum_{d|n}\tau\left(\frac{n}{d}\right)\Psi_d(q).$$

Thus (▼) says

$$\sum_{d|n} q^d \;=\; \sum_{d|n}\tau\left(\frac{n}{d}\right)\Psi_d(q). \tag{3_q}$$

3.4. **Fourth q-identity.** We record another q-identity. The proof relies on Burnside's lemma whose statement we now recall.

Suppose a finite group G acts on a finite set X. Write $G\setminus X$ for the set of G-orbits on X. For $g\in G$, let

$$\chi(g) \;=\; |\{x\in X : g.x = x\}|.$$

Thus $\chi(g)$ counts the number of fixed points of g on X. Burnside's lemma says that the number of G-orbits on X is the average value of χ on G:

$$|G\setminus X| \;=\; \frac{1}{|G|}\sum_{g\in G}\chi(g).$$

We apply Burnside's lemma to the action of $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ on $\mathbb{F}_{q^n}$. To simplify the notation, we set $\Gamma = \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. As noted above, Γ is cyclic of order n with canonical generator Φ where $\Phi(\lambda)=\lambda^q$ for $\lambda\in\mathbb{F}_{q^n}$.

There is a natural bijection

$$\begin{aligned}
\Gamma\setminus\mathbb{F}_{q^n} \quad &\longleftrightarrow \quad \text{set of monic irreducible polynomials} \\
&\qquad\qquad \text{of degree dividing } n \text{ in } \mathbb{F}_q[\mathrm{X}] \\
\Gamma.\alpha \quad &\longleftrightarrow \quad \min\nolimits_{\mathbb{F}_q}\alpha.
\end{aligned}$$

Indeed, for $\alpha\in\mathbb{F}_{q^n}$, the orbit $\Gamma.\alpha$ is precisely the set of roots of $\min_{\mathbb{F}_q}\alpha$ in $\mathbb{F}_{q^n}$. Moreover, as α varies through $\mathbb{F}_{q^n}$, the elements $\min_{\mathbb{F}_q}\alpha$ vary through the set of monic irreducible polynomials in $\mathbb{F}_q[\mathrm{X}]$ of degree dividing n. Thus

$$\begin{aligned}
|\Gamma\setminus\mathbb{F}_{q^n}| \;&=\; \sum_{d|n} N_d(q) \\
&=\; \sum_{d|n}\frac{1}{d}\Psi_d(q).
\end{aligned}$$

Observe next that Γ has $\phi(d)$ elements of order d, namely the generators of the unique subgroup $\langle\Phi^{n/d}\rangle$ of order d. It follows that the set of fixed points for each of these elements is $\mathbb{F}_{q^{n/d}}$, whence

$$\sum_{\gamma\in\Gamma}\chi(\gamma) \;=\; \sum_{d|n}\phi(d)q^{n/d}.$$

Therefore Burnside's lemma gives

$$\sum_{d|n}\frac{1}{d}\Psi_d(q) \;=\; \frac{1}{n}\sum_{d|n}\phi(d)q^{n/d}$$

which we rewrite as

$$\sum_{d|n} \Psi_d(q)\,\frac{n}{d} \;=\; \sum_{d|n} \phi(d)\,q^{n/d}. \tag{4_q}$$

4. More Convolution Identities.

The identities (1_q)–(4_q) are equivalent. We can see this by the strategy of Section 2, that is, by transferring the identities to the ring $\mathcal{C}$ and observing that any one can be obtained from any other by multiplying by a suitable unit.

We write $\Psi_-(q)$ and $\mathsf{e}_-(q)$ for the elements of $\mathcal{C}$ whose values at $n \in \mathbb{N}$ are $\Psi_n(q)$ and q^n, respectively. We can then express (1_q)–(4_q) as the convolution identities

$$\Psi_-(q) \;=\; \mu \star \mathsf{e}_-(q), \tag{$1_{q\star}$}$$

$$\mathsf{e}_-(q) \;=\; \Psi_-(q) \star \mathsf{1}, \tag{$2_{q\star}$}$$

$$\mathsf{e}_-(q) \star \mathsf{1} \;=\; \Psi_-(q) \star \tau, \tag{$3_{q\star}$}$$

$$\Psi_-(q) \star \mathsf{i} \;=\; \phi \star \mathsf{e}_-(q). \tag{$4_{q\star}$}$$

Exactly as in Section 2, we have $(1_{q\star}) \Leftrightarrow (2_{q\star}) \Leftrightarrow (3_{q\star})$. Finally, observe that $(4_{q\star})$ is obtained from $(1_{q\star})$ by multiplying by $\mathsf{i} \in \mathcal{C}^\times$, so that $(1_{q\star})$ and $(4_{q\star})$ are equivalent. In detail,

$$\begin{aligned} \Psi_-(q) = \mu \star \mathsf{e}_-(q) \quad\Longleftrightarrow\quad \Psi_-(q) \star \mathsf{i} \;&=\; \mu \star \mathsf{e}_-(q) \star \mathsf{i} \\ &=\; \phi \star \mathsf{e}_-(q) \quad (\text{as } \phi = \mu \star \mathsf{i}). \end{aligned}$$

5. An unusual ring.

The identities (1_q)–(4_q) hold for arbitrary prime powers. We can therefore regard them as identities in the polynomial ring $\mathbb{Z}[q]$ where we view q now as an indeterminate. Their most natural home, however, is a ring $\mathbb{Z}\langle q\rangle$ which we introduce in this section. We also introduce a related convolution ring $\mathcal{C}_q$ as a habitat for $(1_{q\star})$–$(4_{q\star})$. We'll see that there are natural ring homomorphisms from $\mathbb{Z}\langle q\rangle$ to $\mathbb{Z}$ and from $\mathcal{C}_q$ to $\mathcal{C}$ that carry our q- and $q_\star$-identities to the number-theoretic identities (1)–(3) and $(1_\star)$–$(3_\star)$. In this sense, (1_q)–(3_q) and $(1_{q\star})$–$(3_{q\star})$ are not just analogues of (1)–(3) and $(1_\star)$–$(3_\star)$ but generalizations.

5.1. **The ring $\mathbb{Z}\langle q\rangle$.** As a set,

$$\mathbb{Z}\langle q\rangle \;=\; \{a_1 q + a_2 q^2 + \cdots + a_n q^n : a_1, \ldots, a_n \in \mathbb{Z}, n \in \mathbb{N}\}$$

where q is a symbol. At first glance, $\mathbb{Z}\langle q\rangle$ consists of polynomials in q with integer coefficients and constant term zero and we add elements of $\mathbb{Z}\langle q\rangle$ in this way. Multiplication in $\mathbb{Z}\langle q\rangle$, however, is *not* ordinary multiplication of polynomials. For

$$f(q) = \sum_{i=1}^{m} a_i q^i \;\text{ and }\; g(q) = \sum_{j=1}^{n} b_j q^j,$$

we define

$$(f \star g)(q) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j q^{ij}. \tag{$\star$}$$

In other words, we multiply powers of q via the formula

$$q^i \star q^j = q^{ij} \tag{$\star'$}$$

and extend $\mathbb{Z}$-linearly. Via these operations, $\mathbb{Z}\langle q\rangle$ is a commutative ring with identity. The (multiplicative) identity element is q.

Remark. The ring $\mathbb{Z}\langle q\rangle$—strange perhaps at first sight—is a natural object: it's the semigroup ring with $\mathbb{Z}$-coefficients of the multiplicative semigroup $\mathbb{N}$. In these terms, the ordinary polynomial ring $\mathbb{Z}[\mathrm{X}]$ is the semigroup ring with $\mathbb{Z}$-coefficients of the additive semigroup $\mathbb{Z}_{\geq 0}$ of nonnegative integers. Note that, by uniqueness of prime factorization, the multiplicative semigroup $\mathbb{N}$ is isomorphic to the direct sum of countably many copies of $\mathbb{Z}_{\geq 0}$ (one for each prime). It follows that we can view $\mathbb{Z}\langle q\rangle$ as a polynomial ring with integer coefficients in countably many indeterminates. More precisely, if we list the primes as $p_1, p_2, \ldots$ and write $\mathrm{X}_1, \mathrm{X}_2, \ldots$ for corresponding indeterminates, then the assignment

$$\begin{aligned} q &\longmapsto 1, \\ q^{p_i} &\longmapsto \mathrm{X}_i, \quad i = 1, 2, \ldots, \end{aligned}$$

extends to an isomorphism of rings

$$\mathbb{Z}\langle q\rangle \simeq \mathbb{Z}[\mathrm{X}_1, \mathrm{X}_2, \ldots].$$

The identities (1_q)–(4_q) involve polynomials with integer coefficients and constant term zero, and so can be viewed as identities in $\mathbb{Z}\langle q\rangle$. Indeed, as an abelian group $\mathbb{Z}\langle q\rangle$ coincides with (more pedantically, is canonically isomorphic to) the subgroup of $\mathbb{Z}[q]$ consisting of polynomials with constant term zero. Hence any additive identity between such polynomials transfers to $\mathbb{Z}\langle q\rangle$.

We define a map

$$\mathsf{e} : \mathbb{Z}\langle q\rangle \longrightarrow \mathbb{Z}$$

by $\mathsf{e} = \dfrac{d}{dq}\Big|_{q=1}$. Thus for $f(q) = \sum_{i=1}^{m} a_i q^i \in \mathbb{Z}\langle q\rangle$,

$$\mathsf{e}(f(q)) = \sum_{i=1}^{m} i a_i.$$

Note that e is a homomorphism of rings, that is,

$$\begin{aligned} \mathsf{e}(f(q) + g(q)) &= \mathsf{e}(f(q)) + \mathsf{e}(g(q)), \\ \mathsf{e}(f(q) \star g(q)) &= \mathsf{e}(f(q))\,\mathsf{e}(g(q)), \qquad \text{for } f(q), g(q) \in \mathbb{Z}\langle q\rangle. \end{aligned}$$

The first equation is immediate and the second follows directly from $(\star)$ or $(\star')$.

5.2. **The ring $\mathcal{C}_q$.** We define the convolution ring $\mathcal{C}_q$ alluded to in the introduction to this section. Its underlying set consists of functions from $\mathbb{N}$ to $\mathbb{Z}\langle q\rangle$. We'll write $f_-(q)$ for a typical element, so that the value of $f_-(q)$ at $n \in \mathbb{N}$ is $f_n(q) \in \mathbb{Z}\langle q\rangle$. In particular, we may view $\Psi_-(q)$ and $\mathsf{e}_-(q)$ as elements of $\mathcal{C}_q$.

Addition in $\mathcal{C}_q$ is pointwise addition of functions. We multiply functions via convolution which we'll again denote by $\star$. Thus for $f = f_-(q), g = g_-(q) \in \mathcal{C}_q$,

$$\begin{aligned}(f+g)_n(q) &= f_n(q) + g_n(q),\\ (f\star g)_n(q) &= \sum_{d|n} f_d(q)\star g_{n/d}(q), \qquad n\in\mathbb{N}.\end{aligned}$$

These operations make $\mathcal{C}_q$ into a commutative ring with identity. The (multiplicative) identity element is $\delta_-(q)$ where

$$\delta_n(q) = \begin{cases} q & \text{if } n=1,\\ 0 & \text{otherwise.}\end{cases}$$

The homomorphism $\mathsf{e} : \mathbb{Z}\langle q\rangle \to \mathbb{Z}$ induces the map

$$f_-(q) \longmapsto \mathsf{e}\circ f_-(q) : \mathcal{C}_q \to \mathcal{C}$$

which we'll write simply as

$$\widetilde{\mathsf{e}} : \mathcal{C}_q \to \mathcal{C}.$$

Thus $\widetilde{\mathsf{e}}(f_-(q))$ sends n to $\mathsf{e}(f_n(q))$ for $f_-(q)\in\mathcal{C}_q$, $n\in\mathbb{N}$. From the definitions, we see that $\widetilde{\mathsf{e}} : \mathcal{C}_q \to \mathcal{C}$ is again a homomorphism of rings.

Observe that we can also multiply elements of $\mathcal{C}$ and $\mathcal{C}_q$ via convolution. Explicitly, for $\alpha\in\mathcal{C}$ and $f_-(q)\in\mathcal{C}_q$, the product $\alpha\star f_-(q)$ is given by

$$n \longmapsto \sum_{d|n}\alpha(d)\, f_{n/d}(q), \qquad n\in\mathbb{N}.$$

In this way, $\mathcal{C}_q$ is a module over $\mathcal{C}$. Moreover, if we view $\mathcal{C}$ as a module over itself by convolution (the regular module), then $\widetilde{\mathsf{e}} : \mathcal{C}_q \to \mathcal{C}$ is a $\mathcal{C}$-module homomorphism.

5.3. **$\star$-identities from $q\star$-identities.** We show that $(1_\star)$–$(3_\star)$ follow from $(1_{q\star})$–$(3_{q\star})$ by applying the map $\widetilde{\mathsf{e}}$. The "extra" identity $(4_{q\star})$ plays a crucial role.

For ease of reference, we repeat $(1_{q\star})$–$(4_{q\star})$, interpreted now as identities in the $\mathcal{C}$-module $\mathcal{C}_q$:

$$\Psi_-(q) = \mu\star \mathsf{e}_-(q), \tag{$1_{q\star}$}$$

$$\mathsf{e}_-(q) = \Psi_-(q)\star 1, \tag{$2_{q\star}$}$$

$$\mathsf{e}_-(q)\star 1 = \Psi_-(q)\star\tau, \tag{$3_{q\star}$}$$

$$\Psi_-(q)\star \mathsf{i} = \phi\star \mathsf{e}_-(q). \tag{$4_{q\star}$}$$

We set

$$\widetilde{\mathsf{e}}(\Psi_-(q)) = \psi.$$

Observe that $\widetilde{\mathsf{e}}(\mathsf{e}_-(q)) = \mathsf{i}$. Applying the $\mathcal{C}$-module map $\widetilde{\mathsf{e}} : \mathcal{C}_q \to \mathcal{C}$ to $(1_{q\star})$–$(3_{q\star})$ therefore yields

$$\begin{aligned} \psi &= \mu \star \mathsf{i}, \\ \mathsf{i} &= \psi \star 1, \\ \mathsf{i} \star 1 &= \psi \star \tau. \end{aligned}$$

These are just the identities (1)–(3) with ψ in place of ϕ, so we need to show that $\psi = \phi$. For this, we apply $\widetilde{\mathsf{e}}$ to $(4_{q\star})$ to obtain

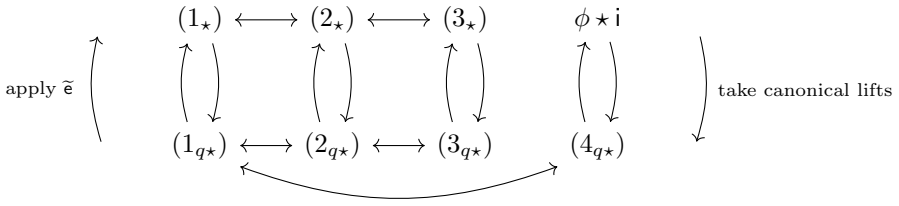
$$\psi \star \mathsf{i} = \phi \star \mathsf{i},$$

whence $\psi = \phi$ (using $\mathsf{i} \in \mathcal{C}^\times$).

6. Multiplicativity and Canonical Lifts.

In this section we show that $(1_{q\star})$–$(3_{q\star})$ follow from the number-theoretic identities $(1_\star)$–$(3_\star)$ via a uniqueness principle. Our approach also yields an alternative proof of $(4_{q\star})$. It hinges on two notions—*multiplicativity* of elements of $\mathcal{C}$ and $\mathcal{C}_q$ and the concept of a *canonical lift* of a multiplicative element of $\mathcal{C}$ to $\mathcal{C}_q$.

The following schematic diagram summarizes the implications we've already noted or will soon establish.



The right and left arrows arise by multiplication by suitable units in $\mathcal{C}$. It remains only to prove the implications from the top to the bottom row.

6.1. **Multiplicativity.** A function $f \in \mathcal{C}$ is *multiplicative* if

- $f(mn) = f(m)f(n)$ for any relatively prime positive integers m and n,
- $f(1) = 1$.

The second condition serves only to exclude the zero function. Indeed, for any f that satisfies the first condition, $f(1) = f(1)f(1)$ and $f(n) = f(1)f(n)$ for all $n \in \mathbb{N}$. Thus $f(1) = 0$ or $f(1) = 1$ and if $f(1) = 0$ then f is identically zero.

We extend the terminology to the ring $\mathcal{C}_q$ and say that $f_-(q) \in \mathcal{C}_q$ is multiplicative if

- $f_{mn}(q) = f_m(q) \star f_n(q)$ for any relatively prime positive integers m and n,
- $f_1(q) = q$.

A multiplicative element of $\mathcal{C}$ or $\mathcal{C}_q$ is determined by its values at prime powers.

It is crucial for our purposes that convolution preserves multiplicativity.

Proposition. *Let $\alpha, \beta \in \mathcal{C}$ and $f_-(q), g_-(q) \in \mathcal{C}_q$ be multiplicative. Then $\alpha \star \beta \in \mathcal{C}$ and $\alpha \star f_-(q), f_-(q) \star g_-(q) \in \mathcal{C}_q$ are also multiplicative.*

Proof. We'll check only that $\alpha \star \beta \in \mathcal{C}$ is multiplicative. The argument in the other cases is effectively identical. Observe first that

$$(\alpha \star \beta)(1) = \alpha(1)\beta(1) = 1 \cdot 1 = 1.$$

Now let m and n be relatively prime positive integers. Any divisor d of mn factors uniquely as $d_1 d_2$ where $d_1 \mid m$ and $d_2 \mid n$. Hence

$$\begin{aligned}
(\alpha \star \beta)(mn) &= \sum_{d \mid mn} \alpha(d)\,\beta(mn/d) \\
&= \sum_{d_1 \mid m} \sum_{d_2 \mid n} \alpha(d_1 d_2)\,\beta(mn/d_1 d_2) \\
&= \sum_{d_1 \mid m} \sum_{d_2 \mid n} \alpha(d_1)\alpha(d_2)\,\beta(m/d_1)\beta(n/d_2) \\
&= \sum_{d_1 \mid m} \alpha(d_1)\,\beta(m/d_1) \cdot \sum_{d_2 \mid n} \alpha(d_2)\,\beta(n/d_2) \\
&= (\alpha \star \beta)(m)\,(\alpha \star \beta)(n).
\end{aligned}$$

□

Corollary. *The functions $\phi, \tau, \sigma \in \mathcal{C}$ and $\Psi_{\_}(q) \in \mathcal{C}_q$ are multiplicative.*

Proof. The functions $\mathsf{1}$ and i are self-evidently multiplicative. Moreover, a moment's thought shows that the Möbius function μ is multiplicative. It follows that $\phi = \mu \star \mathsf{i}$, $\tau = \mathsf{1} \star \mathsf{1}$, and $\sigma = \mathsf{i} \star \mathsf{1}$ are multiplicative. Similarly, $\mathsf{e}_{\_}(q)$ is visibly multiplicative, and so $\Psi_{\_}(q) = \mu \star \mathsf{e}_{\_}(q)$ is multiplicative. □

Example. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of an integer $n > 1$. Multiplicativity of ϕ and its simple form on prime powers gives the familiar formula

$$\begin{aligned}
\phi(n) &= \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r}) \\
&= \left(p_1^{e_1} - p_1^{e_1 - 1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r - 1}\right)
\end{aligned}$$

which is implicit also in equation (c) in Section 1. The parallel formula for $\Psi_n(q) \in \mathbb{Z}\langle q \rangle$ is

$$\begin{aligned}
\Psi_n(q) &= \Psi_{p_1^{e_1}}(q) \star \cdots \star \Psi_{p_r^{e_r}}(q) \\
&= \left(q^{p_1^{e_1}} - q^{p_1^{e_1 - 1}}\right) \star \cdots \star \left(q^{p_r^{e_r}} - q^{p_r^{e_r - 1}}\right).
\end{aligned}$$

Straightforward calculations show that $(1_{q\star})$–$(4_{q\star})$ hold at prime powers. Multiplicativity then implies that they hold at all positive integers. This, however, is an unsatisfactory approach—it fails to explain why the identities *must* hold at prime powers. Instead, we'll establish a uniqueness principle (recorded in the theorem below and its corollary) that makes the identities inevitable at prime powers and hence at all positive integers.

6.2. **Canonical lifts.** The map $\widetilde{\mathsf{e}} : \mathcal{C}_q \to \mathcal{C}$ preserves multiplicativity: if $f_{\_}(q) \in \mathcal{C}_q$ is multiplicative then $\widetilde{\mathsf{e}}(f_{\_}(q)) \in \mathcal{C}$ is multiplicative. In the opposite direction, given a multiplicative $f \in \mathcal{C}$, can we find a multiplicative $f_{\_}(q) \in \mathcal{C}_q$ such that $\widetilde{\mathsf{e}}(f_{\_}(q)) = f$? To facilitate our discussion, we introduce some terminology.

Definition. Let $f \in \mathcal{C}$ be multiplicative. We say that $f_-(q) \in \mathcal{C}_q$ *lifts* f or is a *lift* of f if $f_-(q)$ is multiplicative and $\widetilde{\mathsf{e}}(f_-(q)) = f$.

Thus our question is: does every multiplicative element in $\mathcal{C}$ admit a lift to $\mathcal{C}_q$? Posed in this form, the answer is "yes" for trivial reasons. For example, given $f \in \mathcal{C}$ multiplicative, we can simply set $f_n(q) = f(n)q$ for $n \in \mathbb{N}$. Is there a more intrinsic lift, one that reflects the structure of the ring $\mathbb{Z}\langle q\rangle$? For instance, $\mathsf{e}_-(q)$ and $\Psi_-(q)$ lift i and ϕ, respectively, and are surely the most natural lifts of these elements. What makes them so? Trying to answer this question led us to the following notion.

Definition. Let $f \in \mathcal{C}$ be multiplicative. We say that $f_-(q) \in \mathcal{C}_q$ is a *canonical lift* of f if

- $f_-(q)$ is a lift of f;
- for each prime p and each positive integer k,

$$f_{p^k}(q) = q^p \star f_{p^{k-1}}(q) + c_k q \tag{IC}$$

  for some $c_k \in \mathbb{Z}$.

In the crucial iterative condition (IC), observe that the integers c_k are determined. Indeed, if we apply $\mathsf{e} : \mathbb{Z}\langle q\rangle \to \mathbb{Z}$ to (IC), then

$$f(p^k) \;=\; pf(p^{k-1}) + c_k \;\text{ or }\; c_k = f(p^k) - pf(p^{k-1}).$$

Thus

$$\begin{aligned} f_p(q) \;&=\; q^p + c_1 q \qquad\qquad \text{with } c_1 = f(p) - p, \\ f_{p^2}(q) \;&=\; q^{p^2} + c_1 q^p + c_2 q \qquad \text{with } c_2 = f(p^2) - pf(p), \end{aligned}$$

and so on. In general, with $c_0 = 1$ and $c_j = f(p^j) - pf(p^{j-1})$ for $j \geq 1$ (as above),

$$f_{p^k}(q) \;=\; \sum_{i=0}^{k} c_{k-i}\, q^{p^i}, \quad k = 0, 1, 2, \ldots.$$

Thus a canonical lift is completely determined at prime powers.

Using multiplicativity, it follows that canonical lifts exist and are unique. We are justified so in speaking of *the* canonical lift of a multiplicative element of $\mathcal{C}$.

Example. It's immediate that the multiplicative function $\mathsf{e}_-(q)$ satisfies (IC). In detail, for any prime p and any positive integer k,

$$\mathsf{e}_{p^k}(q) = q^{p^k} = q^p \star q^{p^{k-1}} = q^p \star \mathsf{e}_{p^{k-1}}(q).$$

Hence $\mathsf{e}_-(q)$ is the canonical lift of i.

Similarly, for any prime p and any integer $k \geq 2$,

$$\begin{aligned} \Psi_{p^k}(q) \;&=\; q^{p^k} - q^{p^{k-1}} \\ &=\; q^p \star \left(q^{p^{k-1}} - q^{p^{k-2}}\right) \\ &=\; q^p \star p^{k-1} \Psi_{p^{k-1}}(q). \qquad \text{rem. to delete } p^{k-1} \end{aligned}$$

Further,

$$\begin{aligned}\Psi_p(q) &= q^p - q \\ &= q^p \star \Psi_1(q) - q.\end{aligned}$$

In all, the multiplicative function $\Psi_{\_}(q)$ satisfies (IC) and hence is the canonical lift of ϕ.

6.3. **Canonical lifts and convolution.** The key to our analysis is that canonical lifts commute with convolution.

Theorem. *Let $\alpha, f \in \mathcal{C}$ be multiplicative. Writing $f_{\_}(q)$ and $(\alpha \star f)_{\_}(q)$ for the canonical lifts of f and $\alpha \star f$, respectively, we have*

$$\alpha \star f_{\_}(q) \;=\; (\alpha \star f)_{\_}(q).$$

Proof. The element $\alpha \star f_{\_}(q) \in \mathcal{C}_q$ is a lift of $\alpha \star f \in \mathcal{C}$. To show that it coincides with the canonical lift $(\alpha \star f)_{\_}(q)$, we only have to check that $\alpha \star f_{\_}(q)$ satisfies (IC). To this end, let p be a prime and k be a positive integer. Writing $\alpha \star f_n(q)$ for the value of $\alpha \star f_{\_}(q)$ at n, we have

$$\begin{aligned}\alpha \star f_{p^k}(q) &= \sum_{i=0}^{k} \alpha(p^{k-i})\, f_{p^i}(q) \\ &= \alpha(p^k)\, q + \sum_{i=1}^{k} \alpha(p^{k-i}) \left(q^p \star f_{p^{i-1}}(q) + c_i\, q\right) \\ &= q^p \star \sum_{i=1}^{k} \alpha(p^{k-i}) \star f_{p^{i-1}}(q) + \left(\sum_{i=0}^{k} \alpha(p^{k-i})\, c_i\right) q \\ &= q^p \star \sum_{j=0}^{k-1} \alpha(p^{k-1-j})\, f_{p^j}(q) + \left(\sum_{i=0}^{k} \alpha(p^{k-i})\, c_i\right) q \\ &= q^p \star \left(\alpha \star f_{p^{k-1}}(q)\right) + \gamma_k\, q, \quad \text{for some } \gamma_k \in \mathbb{Z}.\end{aligned}$$

This completes the proof. □

Remark. We can use the theorem to see once more that $\Psi_{\_}(q)$ is the canonical lift of ϕ. Indeed, as noted in the preceding example, $\mathsf{e}_{\_}(q)$ is plainly the canonical lift of i, whence $\Psi_{\_}(q) = \mu \star \mathsf{e}_{\_}(q)$ must be the canonical lift of $\phi = \mu \star \mathsf{i}$.

Corollary. *Let $\alpha, \beta \in \mathcal{C}$ be multiplicative with canonical lifts $\alpha_{\_}(q), \beta_{\_}(q) \in \mathcal{C}_q$. Then*

$$\alpha \star \beta_{\_}(q) \;=\; \alpha_{\_}(q) \star \beta.$$

Proof. Each side is the canonical lift of $\alpha \star \beta \in \mathcal{C}$. □

6.4. **$q\star$-identities from $\star$-identities.** Finally, we use the theorem and its corollary to derive $(1_{q\star})$–$(4_{q\star})$ from $(1_\star)$–$(3_\star)$ and the trivial identity $\phi \star \mathsf{i} = \phi \star \mathsf{i}$.

For convenience, we recapitulate our $\star$-identities:

$$\phi = \mu \star \mathsf{i}, \tag{$1_\star$}$$

$$\mathsf{i} = \phi \star 1, \tag{$2_\star$}$$

$$\sigma = \phi \star \tau. \tag{$3_\star$}$$

We observed a moment ago that ϕ has canonical lift $\Psi_-(q)$ and i has canonical lift $\mathsf{e}_-(q)$. Applying the theorem to $(1_\star)$ and $(2_\star)$ then yields

$$\Psi_-(q) = \mu \star \mathsf{e}_-(q), \tag{$1_{q\star}$}$$

$$\mathsf{e}_-(q) = \Psi_-(q) \star 1. \tag{$2_{q\star}$}$$

Another application of the theorem shows that $\sigma = \mathsf{i} \star 1$ has canonical lift $\mathsf{e}_-(q) \star 1$. On the other hand, $\phi \star \tau$ has canonical lift $\Psi_-(q) \star \tau$ (again by the theorem). Using uniqueness of canonical lifts, we see that $(3_\star)$ implies

$$\mathsf{e}_-(q) \star 1 = \Psi_-(q) \star \tau. \tag{$3_{q\star}$}$$

Now consider the convolution $\phi \star \mathsf{i}$. Taking canonical lifts and applying the corollary, we obtain

$$\Psi_-(q) \star \mathsf{i} = \phi \star \mathsf{e}_-(q). \tag{$4_{q\star}$}$$

Acknowledgements. We are grateful to an anonymous referee and to the Editor, Prof. Colley, for helpful comments and suggestions.

References

[1] Berberian, S. K. (1992). Number-theoretic functions via convolution rings. *Math. Mag.* 65(2): 75–90.
[2] Chebolu, S. K., Mináč, J. (2011). Counting irreducible polynomials over finite fields using the inclusion-exclusion principle. *Math. Mag.* 84(5): 369–371.
[3] Cox, D. (2012). *Galois Theory,* 2nd ed. Hoboken, NJ: John Wiley & Sons.
[4] Delany, J. E. (2005). Groups of arithmetical functions. *Math. Mag.* 78(2): 83–97.
[5] Dummit, D. S., Foote, R. M. (2004). *Abstract Algebra,* 3rd ed. Hoboken, NJ: John Wiley & Sons.
[6] Ireland, K., Rosen, M. (1990). *A Classical Introduction to Modern Number Theory,* 2nd ed. Graduate Texts in Math., 84, New York, NY: Springer-Verlag.
[7] Isaacs, I. M. (1994). *Algebra: A Graduate Course.* Graduate Studies in Math., 100. Providence, RI: American Mathematical Society.
[8] Reid, J. D. (1991). On finite groups and finite fields. *Amer. Math. Monthly.* 98(6): 549–551.

Dept. of Mathematics, University of North Texas, Denton, TX 76203.
E-mail address: Jonathan.Cohen@unt.edu

Dept. of Mathematics, University of Oklahoma, Norman, OK 73019.
E-mail address: aroche@ou.edu