AARMS 5910: q-SERIES IN NUMBER THEORY AND COMBINATORICS

HEESUNG YANG

ABSTRACT. We will develop the theory of combinatorial and analytic identities, summation theorems, and related topics through analytic and combinatorial techniques. The combinatorics involves counting subspaces and mapping vector spaces over finite fields, and partitioning theoretic identities of number theory. The Möbius function on partially ordered sets will also be mentioned.

We will pay special attention to identities like the Rogers-Ramanujan identities and their various generalizations in some detail. A central piece of the analytic development is the Askey–Wilson integral and its generalizations.

Over all the course will be a bridge between analysis and discrete mathematics through the use of combinatorial and analytic tools. The treatment we propose is very conceptual and is a major improvement over the earlier approaches.

The classical approach to q-series is available in [AAR99] and [GR04]. One classic reference on partitions and number theory is [And98].

The lectures will be based on the lecture notes [IS]. A copy of these notes will be made available to the students in the class.

CONTENTS

1. Introduction to q-series 2
2. Theory of integer partitions 3
2.1. Partition functions and their generating functions 3
2.2. Graphical representation of a partition 5
2.3. Partitions fitting in a "box" 5
3. q-binomial theorems and the Jacobi triple product 8
4. Number-theoretic applications of the Jacobi triple product 11
4.1. Sum of two squares theorem 11
4.2. Square, triangular numbers, and pentagonal numbers 14
5. Integer partitions modulo 5 and the Rogers-Ramanujan identities 15
6. Finite fields 19
6.1. Vector space counting 19
6.2. Connection to partitions and the finite q-binomial theorem 20
7. Rogers–Szegő polynomials and q-Hermite polynomials 22
7.1. Interlude: Perfect matching 24
8. Möbius inversion formula 24
8.1. Number-theoretic Möbius inversion formula 25
8.2. Partially ordered sets and incidence algebra 27
8.3. Möbius inversion formula for partially ordered sets 29
9. Möbius functions in special settings 30

Date: 27 July 2019.

9.1. Möbius function for boolean algebras 30
9.2. Möbius function for the subspaces and the q-Möbius inversion formula 32
9.3. Möbius function in number theory, revisited 34
9.4. Convolution in number theory: Dirichlet convolution 35
References 40

1. Introduction to q-series

We shall define a few notations that will be used throughout this course.

Definition 1.1. The *q-Pochhammer symbol* or the *q-shifted factorial* is defined by

$$(a;q)_n := (1-a)(1-aq)(1-aq^2)\cdots(1-aq^{n-1}).$$

More generally, we shall define

$$(a_1,\dots,a_k;q)_n := \prod_{j=1}^{k}(a_j;q)_n$$

and

$$\frac{(q;q)_n}{(1-q)^n} = \frac{(1-q)(1-q^2)\cdots(1-q^n)}{(1-q)^n}.$$

Remark. Observe that

$$\begin{aligned}\lim_{q\to 1^-}\frac{(q;q)_n}{(1-q)^n} &= \lim_{q\to 1^-}\frac{(1-q)(1-q^2)\cdots(1-q^n)}{(1-q)^n}\\ &= \lim_{q\to 1^-}\prod_{k=1}^{n}\frac{1-q^k}{1-q} = \lim_{q\to 1^-}\prod_{k=1}^{n}(1+q+q^2+\cdots+q^{k-1}) = n!.\end{aligned}$$

We also have the q-analogue of the binomial coefficients and the gamma function.

Definition 1.2. The *q-gamma function* is defined by

$$\Gamma_q(x) := \frac{(1-q)^{1-x}(q;q)_\infty}{(q^x;q)_\infty} = (1-q)^{1-x}\prod_{n=0}^{\infty}\frac{1-q^{n+1}}{1-q^{n+x}},$$

provided that $|q|<1$. The *q-binomial coefficient* is defined by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{(q;q)_n}{(q;q)_k(q;q)_{n-k}}.$$

Remark. We have

$$\begin{aligned}\frac{\Gamma_q(x+1)}{\Gamma_q(x)} &= \frac{(1-q)^{-x}}{(1-q)^{1-x}}\cdot\frac{(q^x;q)_\infty}{(q^{x+1};q)_\infty}\\ &= \frac{(1-q^x)(1-q^{x+1})\cdots}{(1-q)(1-q^{x+1})\cdots} = \frac{1-q^x}{1-q}.\end{aligned}$$

Remark. Since expanding the q-binomial coefficient gives

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(1-q)(1-q^2)\cdots(1-q^n)}{(1-q)(1-q^2)\cdots(1-q^k)(1-q)\cdots(1-q^{n-k})},$$

it follows that $\begin{bmatrix} n \\ k \end{bmatrix}_q$ has degree $\binom{n+1}{2} - \binom{k+1}{2} - \binom{n-k+1}{2}$.

2. Theory of integer partitions

2.1. Partition functions and their generating functions

Definition 2.1. The *partition* of an integer n is $(n_1, \ldots, n_k)$ with $n_1 \geq n_2 \geq \cdots \geq n_k$ such that $n_1 + n_2 + \cdots + n_k = n$. The number of partitions of n is denoted by $p(n)$.

Example. There are seven partitions of 5: $5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1$, and $1+1+1+1+1$.

Theorem 2.1 (Euler)**.** $1 + \sum_{n=1}^{\infty} p(n)q^n = \frac{1}{(q;q)_\infty} = \frac{1}{(1-q)(1-q^2)\cdots}$.

Remark. Before we delve into the proofs, we will explore where the singularities are. It is straightforward to see that the given power series is convergent for all $|q| < 1$; but all the roots of unity are singularities, which is a dense subset of the unit circle. So this is a tough function to explore.

Proof. Observe that the RHS is equal to the following infinite product.

$$(1 + q + q^{1+1} + q^{1+1+1} + \cdots)(1 + q^2 + q^{2+2} + q^{2+2+2} + \cdots)\cdots. \tag{2.1}$$

Is it "legal" to write the RHS this way? Yes indeed, as far as computing the coefficient of q^n is concerned. Note that the term we pick from each of $(1+x^k+x^{2k}+\cdots)$ determines how many times the number k shows up in a partition of n as we compute the coefficient of q^n. The number of ways we can pick one term from each of the infinite products $(1+x^k+x^{2k}+\cdots)$ so that the sum of the exponents is equal to n is precisely the number of partitions of n. Hence, the number of partitions of n must be $p(n)$ as required. □

But what if we want to find partitions that only consist of numbers from a set S? In this case, we can use the similar reasoning to see that

$$\sum_{n=1}^{\infty} p_S(n)q^n = \left(\prod_{n\in S}(1-q^n)\right)^{-1},$$

since the infinite product of the form $(1 + q^k + q^{k+k} + \cdots)$ shows up in the RHS only when $k \in S$.

Definition 2.2. We shall denote $P_o(n)$ (resp. $P_d(n)$) the set of partitions of n into odd parts (resp. the set of partitions of n into distinct parts). $p_o(n)$ is defined as the number of partitions of n into odd parts. We shall denote $p_d(n)$ the number of partitions of n into distinct parts.

Example. $p_o(5) = 3$ since $5, 3+1+1$, and $1+1+1+1+1$ are the only available odd partitions of 5.

Proposition 2.1. $1 + \displaystyle\sum_{n=1}^{\infty} p_o(n)q^n = \frac{1}{(1-q)(1-q^3)(1-q^5)\cdots}$.

We can also look into partitions into *distinct parts*. For example, $p_d(5) = 3$ since there are three partitions into distinct parts, namely $5, 4+1, 3+2$.

Proposition 2.2. $1 + \displaystyle\sum_{n=1}^{\infty} p_d(n)q^n = (1+q)(1+q^2)(1+q^3)(1+q^4)\cdots = \prod_{k=1}^{\infty}(1+q^k)$.

Proof. Note that the RHS forces that exactly one of q^k be chosen for any $k \in \mathbb{N}$ when we try to reach q^n via multiplication. □

Theorem 2.2 (Euler)**.** *The number of odd partitions is equal to the number of partitions into distinct parts.*

Combinatorial proof. It is possible to prove this with generating functions, but we will prove this in a combinatorial way by displaying a bijection between the two types of partitions.

Let $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ be a partition of n into distinct parts so that $\lambda_1 > \lambda_2 > \cdots > \lambda_k$. For each λ_i, let $n_i \in \mathbb{N} \cup \{0\}$ satisfy $2^{n_i} \,\|\, \lambda_i$ (i.e., the maximum power of 2 that divides λ_i). We define a function $\Phi : P_d(n) \to P_o(n)$ that does the following for any $\lambda = (\lambda_1, \dots, \lambda_k) \in P_d(n)$:

(1) If λ_i is odd, then leave λ_i as is.
(2) If λ_i is even, then break it into two equal parts (i.e., $\lambda_i = \lambda_i/2 + \lambda_i/2$) until it is impossible to do so.

Note that the once the second step terminates for each of the even parts of $\lambda \in P_d(n)$, there are only odd parts. Furthermore, once this algorithm terminates, for each λ_i, there are exactly 2^{n_i} copies of $\lambda_i' := \lambda_i/2^{n_i}$. Hence,

$$\Phi(\lambda) = (\underbrace{\lambda_1', \dots, \lambda_1'}_{2^{n_1} \text{ times}}, \cdots, \underbrace{\lambda_k', \dots, \lambda_k'}_{2^{n_k} \text{ times}});$$

furthermore, every λ_i' is odd due to the way n_i is defined, so indeed $\Phi(\lambda) \in P_o(n)$ as needed.

To show that this is a bijection, we need to display the inverse map Ψ from $P_o(n)$ to $P_d(n)$. We will construct Ψ in a way that collects the repeating odd parts of $\lambda' \in P_o(n)$ in a specific manner so that the resulting $\Psi(\lambda')$ is in $P_d(n)$. For each odd integer k that shows up in $\lambda' \in P_o(n)$, let r_k be the number of times k shows up in λ'. Suppose that $r_k = 2^{m_{k,1}} + 2^{m_{k,2}} + \cdots + 2^{m_{k,s_k}}$ is the binary expansion of r_k (i.e., $m_{k,i} \neq m_{k,j}$ whenever $i \neq j$). Define Ψ so that for any

$$\lambda' = (\underbrace{\lambda_1', \dots, \lambda_1'}_{r_{\lambda_1'} \text{ times}}, \cdots, \underbrace{\lambda_k', \dots, \lambda_k'}_{r_{\lambda_k'} \text{ times}})$$

with λ_i' all odd, we have

$$\Psi(\lambda') = (2^{m_{\lambda_1',1}}\lambda_1', 2^{m_{\lambda_1',2}}\lambda_1', \dots, 2^{m_{\lambda_1',r_{\lambda_1'}}}\lambda_1', \dots, 2^{m_{\lambda_k',r_{\lambda_k'}}}\lambda_k').$$

It still is not obvious that $\Psi(\lambda')$ is the partition of n into distinct parts. First, $\Psi(\lambda')$ is a partition of n since

$$n = \sum_{j=1}^{k} r_{\lambda_j'}\lambda_j' = \sum_{j=1}^{k}(2^{m_{\lambda_j,1}} + \cdots + 2^{m_{\lambda_j,s_{\lambda_j}}})\lambda_j' = \sum_{j=1}^{k}\sum_{t=1}^{s_{\lambda_j}} 2^{m_{\lambda_j,t}}\lambda_j',$$

which shows that the sum of the integers that show up in $\Psi(\lambda')$ is indeed n. Furthermore, since $m_{\lambda'_j,s} \neq m_{\lambda'_j,t}$ for any $s \neq t$, it follows that any two parts derived from the identical odd part (some λ'_i) cannot be the same. Now suppose that $2^{m_{\lambda'_j,a}}\lambda'_j = 2^{m_{\lambda'_l,b}}\lambda'_l$ for some $j \neq l, a$, and b; without loss of generality, assume $m_{\lambda'_j,a} > m_{\lambda'_l,b}$. Then we have

$$2^{m_{\lambda_j,a}-m_{\lambda'_l,b}} = \lambda'_l/\lambda'_j.$$

Thus the left-hand side is a power of 2, so λ'_l/λ'_j must be a power of 2 as well. However, λ'_l/λ'_j is odd, so it can be some power of 2 only when $\lambda'_l/\lambda'_j = 1$. Hence $\lambda'_j = \lambda'_l$, so it follows that$m_{\lambda'_j,a} = m_{\lambda_l,b}$. This proves that each part of $\Psi(\lambda')$ is distinct as required. Observe that Ψ is the reverse process of Φ, so Ψ is the inverse of Φ we are looking for. The claim follows. □

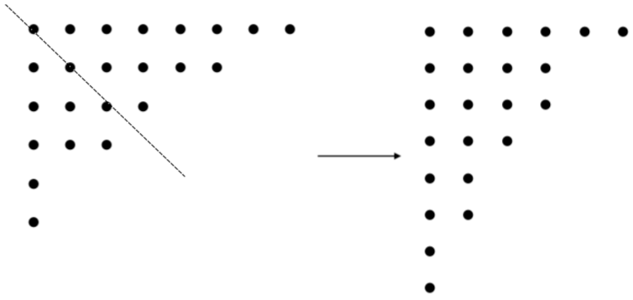
Analytic proof. Observe that

$$1+\sum_{n=1}^{\infty}p_o(n)q^n = \left(\prod_{k=0}^{\infty}(1-q^{2k+1})\right)^{-1} = \prod_{k=1}^{\infty}\frac{1-q^{2k}}{1-q^k} = \prod_{k=1}^{\infty}(1+q^k) = 1+\sum_{n=1}^{\infty}p_d(n)q^n,$$

so it follows that $p_o(n) = p_d(n)$ for any n as required. □

2.2. **Graphical representation of a partition**

One can use the *Ferrers diagram* to represent a partition, by using dots. Such graphical representation gives us one insight regarding partition. Upon flipping the diagram with respect to the diagonal going toward the down-right direction, we are flipping between the largest part and the number of parts, as shown in the diagram below.



If we have a theorem involving the number of parts, we automatically get a theorem involving the largest part, as observed in the above example.

Example. $\dfrac{1}{(1-q)(1-q^2)\cdots(1-q^m)} = 1+\sum f(n)q^n$ where $f(n)$ denotes the number of partition of n whose largest part is at most m. Note that we can replace “whose largest part is at most m” with “whose number of parts is at most m”.

2.3. **Partitions fitting in a “box”**

In the previous section, we looked at the graphical representation of a partition, and from there we could see the bijections between the partitions of n with at most m parts and the partitions of n whose largest part is at most m. First we briefly survey the generating functions for the partition function with only one of the two restrictions (the largest part or the maximum number of parts).

Theorem 2.3. *Let $p_k(n)$ be the number of partitions of n whose largest part is at most k. Then*

$$\sum_{n=0}^{\infty} p_k(n)q^n = \frac{1}{(q;q)_k}.$$

Proof. Apply the similar reasoning as Euler did in Theorem 2.1 while noting that

$$\frac{1}{(q;q)_k} = (1+q+q^{1+1}+\cdots)(1+q^2+q^{2+2}+\cdots)\cdots(1+q^k+q^{k+k}+\cdots). \qquad \square$$

Corollary 2.1. *Suppose that $s_k(n)$ is the number of partitions of n that have at most k parts. Then*

$$\sum_{n=0}^{\infty} s_k(n)q^n = \frac{1}{(q;q)_k}.$$

Proof. Recall that there is a one-to-one correspondence between the number of partitions of a fixed size whose largest part is at most k and partitions that have at most k parts. □

Proposition 2.3. *Let $P_m(n)$ denote the number of partitions of n consisting of* exactly *m parts. Its generating function is*

$$\sum_{n=0}^{\infty} P_m(n)q^n = \frac{q^m}{(q;q)_m}.$$

Proof. It suffices to count how many partitions of n there are whose largest part is exactly m. Thus, we have

$$\begin{aligned}\sum_{n=0}^{\infty} P_m(n)q^n &= \frac{1}{1-q}\frac{1}{1-q^2}\cdots(q^m+q^{2m}+\cdots)\\ &= \frac{q^m}{(1-q)(1-q^2)\cdots(1-q^m)} = \frac{q^m}{(q;q)_m}. \qquad \square\end{aligned}$$

Definition 2.3. Let λ be a partition. Then the *weight* of λ, written $w(\lambda)$ is

$$w(\lambda) = q^s x^t,$$

where s is the size of λ and t is the number of parts of λ.

Theorem 2.4. $(xq;q)_\infty^{-1} = \sum_\lambda w(\lambda) = \sum_{n=0}^{\infty} \frac{q^n x^n}{(q;q)_n}.$

Proof. Observe that

$$\begin{aligned}\frac{1}{(xq;q)_\infty} &= \frac{1}{(1-xq)(1-xq^2)\cdots}\\ &= (1+xq+x^2q^2+\ldots)(1+xq^2+x^2q^{2+2}+\cdots),\end{aligned}$$

so the power of x keeps track of how many parts there are, whereas the power of q keeps track of the size of λ. As for the second equality, note that

$$\sum_\lambda w(\lambda) = \sum_m x^m \cdot \sum_{n=0}^{\infty} P_m(n)q^n,$$

and by Proposition 2.3, we have

$$(xq;q)_\infty^{-1} = \sum_\lambda w(\lambda) = \sum_{m=0}^\infty x^m \frac{q^m}{(q;q)_m},$$

as desired. □

We now shall move towards what we are particularly interested in exploring this section: in the number of partitions of n having both restrictions. In other words, we focus on the partitions of n which fit in, say, a box of dimension $k \times m$ (i.e., a partition's largest part must be at most m, and it must have at most k parts.). Let $f_{m,k}(n)$ be the number of partitions satisfying the desirable condition.

Theorem 2.5. $\displaystyle\sum_{n=0}^\infty f_{m,k}(n)q^n = \begin{bmatrix} m+k \\ k \end{bmatrix}_q.$

Before proving this claim, we will prove the following proposition first.

Proposition 2.4. $\displaystyle\begin{bmatrix} m+k \\ k \end{bmatrix}_q = \begin{bmatrix} m+k-1 \\ k \end{bmatrix}_q + q^m \begin{bmatrix} m+k-1 \\ k-1 \end{bmatrix}_q.$

Proof. The RHS can be re-written using the q-Pochhammer symbols:

$$\begin{aligned} \text{RHS} &= \frac{(q;q)_{m+k-1}}{(q;q)_k(q;q)_{m-1}} + q^m \frac{(q;q)_{m+k-1}}{(q;q)_{k-1}(q;q)_m} \\ &= \frac{(q;q)_{m+k-1}}{(q;q)_k(q;q)_m}\left[1-q^m+q^m(1-q^k)\right] \\ &= \frac{(q;q)_{m+k-1}}{(q;q)_k(q;q)_m}\left[1-q^k\right] = \frac{(q;q)_{m+k}}{(q;q)_k(q;q)_m} = \begin{bmatrix} m+k \\ k \end{bmatrix}_q = \text{LHS}. \end{aligned}$$

□

Proof of Theorem 2.5. Note that any partition fitting into a $k \times m$ box can be broken into two types: first, partitions that fit into the $k \times (m-1)$ box; second, partitions that do not fit into that smaller box. For the sake of simplicity of notation, let $\sum f_{m,k}(n)q^n =: G(m,k)$. Then the generating function for the number of partitions of n fitting into the $k \times (m-1)$ rectangle is precisely $G(m-1,k)$. Observe that any partition of the second type must have the largest part m; upon removing that largest part, the remaining partition necessarily fits into the $(k-1) \times m$ box; the generating function for the number of partitions satisfying such condition is $G(m,k-1)$. But we need to multiply by the factor of q^m to account for the largest part that we removed. Therefore we have $G(m,k) = G(m-1,k) + q^m G(m,k-1)$ for any m and k, so by Proposition 2.4 the claim follows. □

Corollary 2.2. $\displaystyle\frac{1}{(xq;q)_m} = \sum_{k=0}^\infty \begin{bmatrix} m+k-1 \\ k \end{bmatrix}_q q^k x^k.$

Proof. The left-hand side is the generating function for the function that counts all the partitions whose largest part is at most m. Specifically, the coefficient of x^k from the LHS is the generating function of all partitions whose largest part is at most m and have exactly k parts (i.e., fits into a $k \times m$ box). Thus it suffices to argue that $\begin{bmatrix} m+k-1 \\ k \end{bmatrix}_q q^k$ is precisely what we want. Consider any partition that can fit into a $k \times m$ box. Removing the left column, which must have exactly k elements, gives an arbitrary partition that fits into a $k \times (m-1)$ box. The generating function of all partitions satisfying such condition is $\begin{bmatrix} m+k-1 \\ k \end{bmatrix}_q$, as observed in the proof of Theorem 2.5. We multiply $\begin{bmatrix} m+k-1 \\ k \end{bmatrix}_q$ by q^k to account for the first column with k elements we separated from the original partition. □

Since there can be at most mk objects in the $k \times m$ box, it follows that the degree of $\sum f_{m,k}(n)q^n$ is mk. Thus the degree of $\begin{bmatrix} m+k \\ k \end{bmatrix}_q$ is mk as well. Also, for any n, we have $f_{m,k}(n) = f_{m,k}(mk-n)$, since there is a one-to-one correspondence between a partition of n in an $k \times m$ box and the "complement" of that partition (i.e., at any spot that didn't have an object, put an object and vice versa), which gives a partition for $mk - n$ that fit in an $k \times m$ box.

3. q-binomial theorems and the Jacobi triple product

Key tools in partition theory include the q-binomial theorems and the Jacobi triple product, which we need to develop before proving the Rogers-Ramanujan identities, which give insights on the partitions consisting of integers from 1 or 4 modulo 5 (the first identity) or from 2 or 3 modulo 5 (the second identity). In this section we will develop and prove these tools.

Theorem 3.1 (q-binomial theorem, finite version)**.** $(-xq;q)_m = \sum_{k=0}^{m} \begin{bmatrix} m \\ k \end{bmatrix}_q q^{\binom{k+1}{2}} x^k.$

Proof. Since

$$(-xq;q)_m = (1+xq)(1+xq^2)\cdots(1+xq^m),$$

the coefficient of x^k denotes the number of partitions into k distinct parts with the largest part at most m. Let $\lambda = (\lambda_1, \dots, \lambda_k)$ be a partition with k distinct parts whose largest part is at most m, and let $\mu = (\lambda_1 - k, \lambda_2 - (k-1), \dots, \lambda - k - 1 - 2, \lambda_k - 1)$ be the new partition. The largest part must be at most $m-k$, so μ fits in a $k \times (m-k)$ box. The generating function of any such partitions is $\begin{bmatrix} m \\ k \end{bmatrix}_q$; $q^{\binom{k+1}{2}}$ needs to be multiplied to add back the $1 + 2 + \cdots + k = \binom{k+1}{2}$ elements we removed from λ in order to create μ. □

Remark. Notice that if $q = 1$, then we get the regular binomial theorem.

Theorem 3.2 (q-binomial theorem, infinite version)**.** $(-xq;q)_\infty = \sum_{k=0}^{\infty} \frac{q^{\binom{k+1}{2}} x^k}{(q;q)_k}.$

Proof. Since

$$(-xq;q)_\infty = (1+qx)(1+q^2x)\cdots(1+q^nx)\cdots,$$

the coefficient of x^k in $(-xq;q)_\infty$ contains $q^{1+2+\cdots+k} = q^{\binom{k+1}{2}}$ and q^{N_k}, where N_k denotes the number of partitions with at most k parts.

Observe that $\binom{k+1}{2} = 1 + 2 + \cdots + k$, so once you add 1 in the kth part, 2 in the $(k-1)$th part, $\dots$, k in the first part, then we guarantee that each part is distinct. The exponent of x keeps track of how many parts there are; the $(q;q)_k^{-1}$ is responsible for counting how many partitions with k parts there are (no restrictions on the largest part), per Corollary 2.1. □

Theorem 3.3 (Jacobi triple product)**.** $(q;q)_\infty(-z;q)_\infty\left(-\frac{q}{z};q\right)_\infty = \sum_{n=-\infty}^{\infty} q^{\binom{n+1}{2}}z^n.$

Proof. We will start by looking at the following product:

$$\begin{aligned}
(-z;q)_N\left(-\frac{q}{z};q\right)_N &= \left(1+\frac{q}{z}\right)\left(1+\frac{q^2}{z}\right)\cdots\left(1+\frac{q^N}{z}\right)(-z;q)_N \\
&= \frac{1}{z^N}q^{\binom{N+1}{2}}(1+q^{-N}z)\cdots(1+q^{-1}z)(1+z)(1+qz)\cdots(1+q^{N-1}z) \\
&= \frac{1}{z^N}q^{\binom{N+1}{2}}(-zq^{-N};q)_{2N} \\
&\overset{*}{=} \frac{1}{z^N}q^{\binom{N+1}{2}}\sum_{k=0}^{2N}\begin{bmatrix}2N\\k\end{bmatrix}_q (zq^{-N})^k q^{\binom{k}{2}} \\
&\overset{\dagger}{=} q^{\binom{N+1}{2}}\sum_{j=-N}^{N}\frac{(q;q)_{2N}z^j q^{-N(N+j)}}{(q;q)_{N+j}(q;q)_{N-j}}q^{\binom{N+j}{2}},
\end{aligned}$$

where $\overset{*}{=}$ follows from Theorem 3.1, and $\overset{\dagger}{=}$ follows upon replacing k with $N+j$.

Now let's look at the power of q for each individual term. Our calculations show that the power of q is

$$\frac{N(N+1)}{2} - N^2 - Nj + \frac{(N+j)^2}{2} - \frac{N+j}{2} = \frac{j(j+1)}{2}.$$

Now letting $N\to\infty$ gives us

$$\left(-z,-\frac{q}{z};q\right)_\infty = \frac{1}{(q;q)_\infty}\sum_{j=-\infty}^{\infty} q^{\binom{j+1}{2}}z^j. \qquad \square$$

We also present an alternative form of the Jacobi triple product identity.

Theorem 3.4 (Jacobi triple product II)**.** $(q^2;q^2)_\infty(-zq;q^2)_\infty(-z^{-1}q;q^2)_\infty = \sum_{n=-\infty}^{\infty} q^{n^2}z^n.$

Proof. We will start by looking at the following product:

$$\begin{aligned}
(-zq;q^2)_N\left(-\frac{q}{z};q^2\right)_N &= \left(1+\frac{q}{z}\right)\left(1+\frac{q^3}{z}\right)\cdots\left(1+\frac{q^{2N-1}}{z}\right)(-zq;q^2)_N \\
&= (1+q^{-(2N-1)}z)\cdots(1+q^{-1}z)(1+qz)(1+q^3z)\cdots(1+q^{2N-1}z) \\
&= \frac{1}{z^N}(z+q^{2N-1})\cdots(z+q)(1+qz)\cdots(1+q^{2N-1}z) \\
&= \frac{1}{z^N}\left[\prod_{k=1}^{N}q^{-(2k-1)}(q^{-(2k-1)}z+1)\right](z+q)(1+qz)\cdots(1+q^{2N-1}z) \\
&= \frac{1}{z^N}q^{N^2}(-zq^{-(2N-1)};q^2)_{2N} \\
&\overset{*}{=} \frac{1}{z^N}q^{N^2}\sum_{k=0}^{2N}\frac{(q^2;q^2)_{2N}}{(q^2;q^2)_k(q^2;q^2)_{2N-k}}(zq^{-(2N-1)})^k q^{2\binom{k}{2}}
\end{aligned}$$

$$\overset{\dagger}{=} q^{N^2} \sum_{j=-N}^{N} \frac{(q^2;q^2)_{2N} z^j q^{-(2N-1)(N+j)}}{(q^2;q^2)_{N+j}(q^2;q^2)_{N-j}} (q^2)^{\binom{N+j}{2}},$$

where $\overset{*}{=}$ follows from Theorem 3.1, and $\overset{\dagger}{=}$ follows upon replacing k with $N+j$.

Now let's look at the power of q for each individual term. Our calculations show that the power of q is

$$N^2 - (2N-1)(N+j) + (N+j)^2 - (N+j) = j^2.$$

Now letting $N \to \infty$ gives us

$$\left(-zq, -\frac{q}{z}; q^2\right)_\infty = \frac{1}{(q^2;q^2)_\infty} \sum_{j=-\infty}^{\infty} q^{j^2} z^j. \qquad \square$$

We finish this section with the general non-terminating version of the q-binomial theorem.

Theorem 3.5 (General q-binomial theorem). $\dfrac{(qax;q)_\infty}{(qx;q)_\infty} = \displaystyle\sum_{k=0}^{\infty} q^k x^k \frac{(a;q)_k}{(q;q)_k}.$

Proof. By Theorem 3.1, upon replacing x with $-a/q$ we have

$$\frac{(a;q)_m}{(q;q)_m} = \sum_{k=0}^{m} \frac{q^{\binom{k}{2}}(-a)^k}{(q;q)_k(q;q)_{m-k}}.$$

But then note that if

$$a_k := \frac{q^{\binom{k}{2}}(-a)^k}{(q;q)_k} \text{ and } b_k := \frac{1}{(q;q)_k},$$

then

$$c_n := \frac{(a;q)_n}{(q;q)_n} = \sum_{k=0}^{n} a_k b_{n-k}.$$

Thus we have

$$\sum_{k=0}^{\infty} c_k x^k = \left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{k=0}^{\infty} b_k x^k\right)$$

$$\sum_{k=0}^{\infty} \frac{(a;q)_k}{(q;q)_k} x^k = \left(\sum_{k=0}^{\infty} \frac{q^{\binom{k}{2}}(-ax)^k}{(q;q)_k}\right)\left(\sum_{k=0}^{\infty} \frac{1}{(q;q)_k} x^k\right)$$

$$\sum_{k=0}^{\infty} \frac{(a;q)_k}{(q;q)_k} x^k = (ax;q)_\infty \left(\sum_{k=0}^{\infty} \frac{1}{(q;q)_k} x^k\right)$$

by Theorem 3.2. Finally, by Theorem 2.4 (replace x from the statement with xq^{-1}), it follows that

$$\sum_{k=0}^{\infty} \frac{(a;q)_k}{(q;q)_k} x^k = (ax;q)_\infty \left(\sum_{k=0}^{\infty} \frac{1}{(q;q)_k} x^k\right) = \frac{(ax;q)_\infty}{(x;q)_\infty}.$$

The theorem follows upon replacing x with qx. $\square$

4. Number-theoretic applications of the Jacobi triple product

In this section we will explore the application of the Jacobi triple product in combinatorial number theory.

4.1. **Sum of two squares theorem**

Recall that the product rule implies that, for functions $\{f_j\}$,

$$\frac{d}{dx}\log\left(\prod_j f_j\right) = \sum_j \frac{f_j'}{f_j} = \frac{\frac{d}{dx}(\prod f_j)}{\prod f_j}. \tag{4.1}$$

This observation be useful in proving the following theorem.

Theorem 4.1. $\left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^2 = 1 + 4\left[\sum_{n=0}^{\infty} \frac{q^{4n+1}}{1-q^{4n+1}} - \sum_{n=0}^{\infty} \frac{q^{4n+3}}{1-q^{4n+3}}\right].$

Remark. We first examine what the LHS and the RHS each represent. Note that every term in the left-hand side will consist of sum of two squares. Now try to expand the right-hand side first and observe that

$$\frac{q^{4n+1}}{1-q^{4n+1}} = q^{4n+1}(1 + q^{4n+1} + q^{2(4n+1)} + \cdots) = \sum_{j=0}^{\infty} q^j c(j),$$

where $c(j)$ denotes the number of divisors of j that are congruent to 1 mod 4. Similarly

$$\frac{q^{4n+3}}{1-q^{4n+3}} = q^{4n+3}(1 + q^{4n+3} + q^{2(4n+3)} + \cdots) = \sum_{j=0}^{\infty} q^j c'(j),$$

where $c'(j)$ denotes the number of divisors of j that are congruent to 3 mod 4.

Proof. We start from

$$\left(1-\frac{1}{z^2}\right)\left(q, qz^2, \frac{q}{z^2}; q\right) = \left(q, qz^2, \frac{1}{z^2}; q\right)_\infty,$$

and we apply Theorem 3.4 (let $Z := -\sqrt{q}z^2$ and $Q := \sqrt{q}$):

$$\begin{aligned}\left(q, qz^2, \frac{1}{z^2}; q\right)_\infty &= (Q^2, -ZQ, -QZ^{-1}; Q^2)_\infty = \sum_{n=-\infty}^{\infty} Q^{n^2} Z^n \\ &= \sum_{n=-\infty}^{\infty} q^{n^2/2}(-1)^n z^{2n} q^{n/2} = \sum_{n=-\infty}^{\infty} q^{\binom{n+1}{2}}(-1)^n z^{2n}.\end{aligned}$$

Break the last summand into even ($n = 2k$) and odd ($n = 2k-1$):

$$\begin{aligned}\sum_{n=-\infty}^{\infty} q^{\binom{n+1}{2}}(-1)^n z^{2n} &= \sum_{k=-\infty}^{\infty} q^{\binom{2k+1}{2}} z^{4k} - \sum_{k=-\infty}^{\infty} q^{\binom{2k}{2}} z^{4k-2} \\ &= \sum_{k=-\infty}^{\infty} q^{k(2k+1)} z^{4k} - z^{-2}\sum_{k=-\infty}^{\infty} q^{k(2k-1)} z^{4k}\end{aligned}$$

$$\overset{\dagger}{=} \sum_{k=-\infty}^{\infty} q^{k(2k+1)} z^{4k} - z^{-2} \sum_{k=-\infty}^{\infty} q^{k(2k+1)} z^{4k}.$$

Note that $\overset{\dagger}{=}$ holds since, via the change of variable $k \to -k$, i.e.,

$$\sum_{k=-\infty}^{\infty} q^{k(2k-1)} z^{4k} = \sum_{k=-\infty}^{\infty} q^{-k(-2k-1)} z^{-4k} = \sum_{k=-\infty}^{\infty} q^{k(2k+1)} z^{4k}.$$

Apply Theorem 3.4 again to the summand, $q^{k(2k+1)} z^{4k}$:

$$\begin{aligned} \sum_{k=-\infty}^{\infty} q^{k(2k+1)} z^{4k} &= \sum_{k=-\infty}^{\infty} (q^2)^{k^2} (z^4 q)^k \\ &= ((q^2)^2, -(q^2)(qz^4), -(q^2)/(qz^4); (q^2)^2)_\infty \\ &= \left(q^4, -q^3 z^4, -\frac{q}{z^4}; q^4\right)_\infty . \end{aligned}$$

Notice that using our observation (4.1) gives

$$\begin{aligned} \left.\frac{d}{dz}\right|_{z=1} (-cz^4; q^4)_\infty &= (-cz^4; q^4)_\infty \left.\frac{d}{dz}\right|_{z=1} \log(-cz^4; q^4)_\infty \\ &= (-c; q^4)_\infty \sum_{n=0}^{\infty} \left.\frac{4cz^3 q^{4n}}{1 + cz^4 q^{4n}}\right|_{z=1} \\ &= 4(-c; q^4)_\infty \sum_{n=0}^{\infty} \frac{cq^{4n}}{1 + cq^{4n}}. \end{aligned} \tag{4.2}$$

Using the identity (4.2) on the $(q^4, -q^3 z^4, -qz^{-4}; q^4)_\infty$ gives us

$$\left.\frac{d}{dz}\right|_{z=1} \left(q^4, -q^3 z^4, -\frac{q}{z^4}; q^4\right)_\infty = 4(q^4, -q, -q^3; q^4)_\infty \left[\sum_{n=0}^{\infty} \frac{q^{4n+3}}{1 + q^{4n+3}} - \sum_{n=0}^{\infty} \frac{q^{4n+1}}{1 + q^{4n+1}}\right] =: A.$$

Thus

$$\begin{aligned} &\left.\frac{d}{dz}\right|_{z=1} \left[\left(q^4, -q^3 z^4, -\frac{q}{z^4}; q^4\right)_\infty - z^{-2} \left(q^4, -q^3 z^4, -\frac{q}{z^4}; q^4\right)_\infty\right] \\ &= A + 2(q^4, -q^3, -q; q^4)_\infty - (-A) = 2A + 2(q^4, -q^3, -q; q^4)_\infty. \end{aligned} \tag{4.3}$$

On the other hand, since $(1; q)_\infty = 0$, it follows

$$\begin{aligned} \left.\frac{d}{dz}\right|_{z=1} (q; q)_\infty (qz^2; q)_\infty (z^{-2}; q)_\infty &= (q; q)_\infty (q \cdot 1^2; q)_\infty \left[\left.\frac{d}{dz}\right|_{z=1} (z^{-2}; q)_\infty\right] \\ &= (q; q)_\infty^2 \left.\left[\left\{(2z^{-3}) \prod_{j=1}^{\infty} (1 - q^j z^{-2})\right\} + (1 - z^{-2})(\cdots)\right]\right|_{z=1} \\ &= 2(q; q)_\infty^3. \end{aligned} \tag{4.4}$$

Combining (4.3) and (4.4) gives

$$\frac{(q;q)_\infty^3}{(q^4,-q,-q^3;q^4)_\infty} = 4\sum_{n=0}^{\infty}\left[\frac{q^{4n+3}}{1+q^{4n+3}} - \frac{q^{4n+1}}{1+q^{4n+1}}\right] + 1. \tag{4.5}$$

The LHS of (4.5) can be further simplified, since $(-q,-q^3;q^4)_\infty = (-q;q^2)_\infty$. (Note that the product $(-q,-q^3;q^4)_\infty$ is equal to the product $\prod_{k \text{ odd}}(1+q^k)$.) Also, note that we can split $(q;q)_\infty$ into the product of even powers and odd powers, i.e.,

$$(q;q)_\infty = \prod_{k \text{ odd}}(1+q^k)\prod_{\substack{k \text{ even} \\ k\geq 2}}(1+q^k) = (q,q^2;q^2)_\infty.$$

Thus, we have

$$\frac{(q;q)_\infty^3}{(q^4,-q,-q^3;q^4)_\infty} = \frac{(q,q^2;q^2)_\infty^3}{(q^2,-q^2;q^2)_\infty(-q;q^2)_\infty} = \frac{(q;q^2)_\infty^3(q^2;q^2)_\infty^2}{(-q,-q^2;q^2)_\infty} = \frac{(q;q^2)_\infty^3(q^2;q^2)_\infty^2}{(-q;q)_\infty}.$$

But by the analytic proof of Theorem 2.2, we have $(-q;q)_\infty = (q;q^2)_\infty^{-1}$, so

$$\frac{(q;q^2)_\infty^3(q^2;q^2)_\infty^2}{(-q;q)_\infty} = (q;q^2)_\infty^4(q^2;q^2)_\infty^2 = (q^2,q,q;q^2)_\infty^2.$$

Now performing a change of variable (from q to $-q$) gives us

$$(q^2,-q,-q;q^2)_\infty^2 = 1 + 4\sum_{n=0}^{\infty}\left[\frac{q^{4n+1}}{1-q^{4n+1}} - \frac{q^{4n+3}}{1-q^{4n+3}}\right].$$

But then applying the Jacobi triple product (Theorem 3.4) on the left-hand side gives us

$$(q^2,-q,-q;q^2)_\infty^2 = \left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^2,$$

so the proof is complete. □

Definition 4.1. We will denote $r_k(n)$ the number of ways to write n as a sum of k squares.

We will count in how many ways, say, we can write 17 as a sum of two squares. There are eight ways (we count a partition with different signs as distinct; a^2+b^2 and b^2+a^2 are also considered distinct): $1^2+4^2, (-1)^2+(-4)^2, 1^2+(-4)^2, (-1)^2+4^2, 4^2+1^2, (-4)^2+(-1)^2, (-4)^2+1^2, 4^2+(-1)^2$. Therefore, $r_2(17) = 8$.

Theorem 4.2 (Jacobi)**.** *Let $d_j(n)$ denote the number of divisors of n that are congruent to j mod 4. Then $r_2(n) = 4(d_1(n) - d_3(n))$ for all $n \geq 1$.*

Proof. Evidently, we have

$$\left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^2 = 1 + \sum_{n=1}^{\infty} r_2(n)q^n,$$

and thanks to Theorem 4.1, we have

$$1 + \sum_{n=1}^{\infty} r_2(n)q^n = 1 + 4\sum_{n=0}^{\infty}\left[\frac{q^{4n+1}}{1-q^{4n+1}} - \frac{q^{4n+3}}{1-q^{4n+3}}\right] = 1 + 4\sum_{n=0}^{\infty}\sum_{k=1}^{\infty}[q^{k(4n+1)} - q^{k(4n+3)}].$$

Note that q^n will appear from each summand in the right-hand side if and only if n can be written in the form $n = dn'$ where $d \equiv 1$ or $3 \bmod 4$; and since the coefficient of each power is ± 1, it follows that each factor of n congruent to $1 \bmod 4$ will contribute 1 toward the coefficient of q^n whereas each factor of n congruent to $3 \bmod 4$ will contribute -1 toward the coefficient of q^n. Therefore, we indeed have

$$1 + 4\sum_{n=0}^{\infty}\sum_{k=1}^{\infty}[q^{k(4n+1)} - q^{k(4n+3)}] = 1 + 4\sum_{n=1}^{\infty}(d_1(n) - d_3(n))q^n,$$

so indeed $r_2(n) = 4(d_1(n) - d_3(n))$ for all $n \geq 1$ as required. □

Example. Consider $n = 10$. There are four divisors: $1, 2, 5, 10$. Then $d_3(10) = 0$ and $d_1(10) = 2$. So by the theorem above, there are 8 ways to write 10 as a sum of two squares: $(-1)^2 + 3^2, 3^2 + (-1)^2, (-1)^2 + (-3)^2, (-3)^2 + (-1)^2, 1^2 + 3^2, 3^2 + 1^2, 1^2 + (-3)^2, (-3)^2 + 1^2$.

This gives us a combinatorial proof of the following theorem, which one encounters at the beginning of algebraic number theory (in the context of $\mathbb{Z}[i]$, the ring of Gaussian integers).

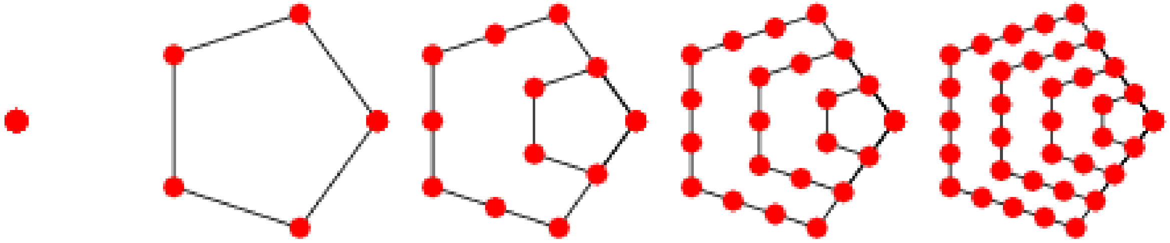
Theorem 4.3. *Let p be a prime. Then p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$.*

Proof. If $p \equiv 1 \pmod 4$, then $d_1(p) = 2$ (namely, 1 and itself) whereas $d_3(p) = 0$. Thus $r_2(p) = 8$. On the other hand, if $p \equiv 3 \pmod 4$, then $d_1(p) = 1$ (namely, 1) and $d_3(p) = 1$ (namely, p itself). Thus in this case, $r_2(p) = 4(1 - 1) = 0$, so p cannot be written as a sum of two squares. □

4.2. **Square, triangular numbers, and pentagonal numbers**

Definition 4.2. Any number that is the of the integers between 1 and n inclusive is called a *triangular number.* Thus, any triangular number is of the form $\binom{n}{2}$.

Definition 4.3. If n objects can be arranged in a regular pentagonal shape, then n is a *pentagonal number.* Any pentagonal number is of the form $\frac{3n^2-n}{2}$.



Theorem 4.4 (Euler pentagonal number theorem)**.** $(q;q)_\infty = \displaystyle\sum_{n=-\infty}^{\infty} q^{(3n^2-n)/2}(-1)^n$.

Proof. By the Jacobi triple product (Theorem 3.4),

$$\sum_{n=-\infty}^{\infty} q^{n^2}(-z)^n = (q^2, qz, q/z; q^2)_\infty.$$

Let $q = p^{3/2}$ and $z = p^{1/2}$. Then

$$\sum_{n=-\infty}^{\infty} p^{3n^2/2}(-1)^n p^{-n/2} = (p^3, p, p^2; p^3)_\infty = (p;p)_\infty.$$ □

5. Integer partitions modulo 5 and the Rogers-Ramanujan identities[1]

Theorem 5.1 (Rogers-Ramanujan identity I). *We have*

$$1+\sum_{k=1}^{\infty}\frac{q^{k^2}}{(q;q)_k}=\prod_{k=0}^{\infty}\frac{1}{(1-q^{5k+1})(1-q^{5k+4})}=\frac{1}{(q,q^4;q^5)_\infty} \tag{5.1}$$

Therefore, there is a bijection between the set of partitions of n whose difference between consecutive parts is at least 2 and the set of partitions of n whose parts consist entirely of integers congruent to 1 or 4 mod 5.

Theorem 5.2 (Rogers-Ramanujan identity II). *We have*

$$1+\sum_{k=1}^{\infty}\frac{q^{k^2+k}}{(q;q)_k}=\prod_{k=0}^{\infty}\frac{1}{(1-q^{5k+2})(1-q^{5k+3})}=\frac{1}{(q^2,q^3;q^5)_\infty}. \tag{5.2}$$

Therefore, there is a bijection between the set of partitions of n whose difference between consecutive parts is at least 2 and whose every part is at least 2 and the set of partitions of n whose parts consist entirely of integers congruent to 2 or 3 mod 5.

There are dozen available proofs of these remarkable identities, but none of them too "simple" and "straightforward". Indeed, Hardy's famous comment remains valid: "None of the proofs of [the Rogers-Ramanujan identities] can be called 'simple' or 'straightforward' [...]; and no doubt it would be unreasonable to expect a really easy proof" [Har40]. One may try to draw a bijection between these two sets of partitions of different nature to prove this. This is indeed possible, as demonstrated by [BP06], but the construction of the bijection is rather elaborate and indeed is far from "simple" or "straightforward".

Before proving these identities, we will define

$$G_i(z;q):=\sum_{n=0}^{\infty}\frac{(-1)^n z^{2n}q^{\frac{1}{2}n(5n+3)-in}(1-z^{i+1}q^{(2n+1)(i+1)})}{(q;q)_n\prod_{j=n+1}^{\infty}(1-zq^j)}$$

and prove the following lemma about $G_i(z;q)$.

Lemma 5.1. *We have*

(1) $G_1(z;q)=G_0(z;q)+zqG_0(zq;q)$,
(2) $G_{-1}(z;q)=0$, *and*
(3) $G_0(z;q)=G_1(zq;q)$.

Proof. For the first claim, note that

$$G_1(z;q)-G_0(z;q)=\sum_{n=0}^{\infty}\frac{(-1)^n z^{2n}q^{\frac{1}{2}n(5n+3)}(q^{-n}-z^2q^{3n+2}-1+zq^{2n+1})}{(q;q)_n\prod_{j=n+1}^{\infty}(1-zq^j)}$$

[1] During the lecture, only the significance of the left-hand side was explained; the proof was not covered until later in the course during the analysis lecture. I gave a more elementary proof in this note, based on Sections 13-2 and 14-1 of [And71].

$$
\begin{aligned}
&= \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)}(q^{-n}(1-q^n) + zq^{2n+1}(1-zq^{n+1}))}{(q;q)_n \prod_{j=n+1}^{\infty}(1-zq^j)} \\
&\overset{*}{=} \sum_{n=1}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)} q^{-n}(1-q^n)}{(q;q)_n \prod_{j=n+1}^{\infty}(1-zq^j)} + \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)} zq^{2n+1}(1-zq^{n+1})}{(q;q)_n \prod_{j=n+1}^{\infty}(1-zq^j)} \\
&\overset{\dagger}{=} \sum_{n=0}^{\infty} \frac{(-1)^{n+1} z^{2n+2} q^{\frac{1}{2}(n+1)(5n+8)} q^{-n-1}}{(q;q)_n \prod_{j=n+2}^{\infty}(1-zq^j)} + \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)} zq^{2n+1}}{(q;q)_n \prod_{j=n+2}^{\infty}(1-zq^j)}.
\end{aligned}
$$

Note that in $\overset{*}{=}$ we changed the starting index of the first sum from $n = 0$ to $n = 1$: this is justified since $1 - q^n = 0$ when $n = 0$. In $\overset{\dagger}{=}$, we changed the variable of the first sum from n to $n + 1$. Now pulling zq from each of the two sums gives

$$
\begin{aligned}
G_1(z;q) - G_0(z;q) &= zq \left(\sum_{n=0}^{\infty} \frac{(-1)^{n+1} z^{2n+1} q^{\frac{1}{2}(n+1)(5n+8)} q^{-n-2}}{(q;q)_n \prod_{j=n+2}^{\infty}(1-zq^j)} + \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)} q^{2n}}{(q;q)_n \prod_{j=n+2}^{\infty}(1-zq^j)} \right) \\
&= zq \sum_{n=0}^{\infty} \frac{(-1)^n (zq)^{2n} q^{\frac{1}{2}n(5n+3)}(1-(zq)q^{2n+1})}{(q;q)_n \prod_{j=n+1}^{\infty}(1-(zq)q^j)} \\
&= zqG_0(zq;q).
\end{aligned}
$$

Therefore $G_1(z;q) = G_0(z;q) + zqG_0(zq;q)$. The second claim is immediate, since if $i = -1$, then

$$
1 - z^{i+1} q^{(2n+1)(i+1)} = 1 - z^0 q^0 = 0.
$$

As for the third claim, using the similar type of argument (with $\overset{*}{=}$ and $\overset{\dagger}{=}$ each marking the step where the same operation as described previously is being used), we see that

$$
\begin{aligned}
G_0(z;q) - G_{-1}(z;q) &= \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)}(1 - zq^{2n+1} - q^n + q^n)}{(q;q)_n \prod_{j=n+1}^{\infty}(1-zq^j)} \\
&= \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)}(1 - q^n + q^n(1-zq^{n+1}))}{(q;q)_n \prod_{j=n+1}^{\infty}(1-zq^j)} \\
&\overset{*}{=} \sum_{n=1}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)}(1-q^n)}{(q;q)_n \prod_{j=n+1}^{\infty}(1-zq^j)} + \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)} q^n(1-zq^{n+1})}{(q;q)_n \prod_{j=n+1}^{\infty}(1-zq^j)} \\
&\overset{\dagger}{=} \sum_{n=0}^{\infty} \frac{(-1)^{n+1} z^{2n+2} q^{\frac{1}{2}(n+1)(5n+8)}}{(q;q)_n \prod_{j=n+2}^{\infty}(1-zq^j)} + \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)} q^n}{(q;q)_n \prod_{j=n+2}^{\infty}(1-zq^j)}
\end{aligned}
$$

$$= \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n} q^{\frac{1}{2}n(5n+3)+n}(1-z^2q^{4n+4})}{(q;q)_n \prod_{j=n+1}^{\infty}(1-(zq)q^j)}$$

$$= \sum_{n=0}^{\infty} \frac{(-1)^n (zq)^{2n} q^{\frac{1}{2}n(5n+3)-n}(1-(zq)^2q^{2(2n+1)})}{(q;q)_n \prod_{j=n+1}^{\infty}(1-(zq)q^j)} = G_1(zq;q).$$

But since $G_{-1}(z;q) = 0$, it follows that $G_0(z;q) = G_1(zq;q)$. □

Proof of Rogers-Ramanujan I. Start with the left-hand side. Suppose that $(x_1, \dots, x_k)$ (as always, assume $x_1 \geq x_2 \geq \cdots \geq x_k$) is a partition whose difference between two consecutive parts is at least 2. Since $x_k \geq 1$, it follows that there is a set of non-negative integers $(y_1, \dots, y_k)$ such that $(y_1, \dots, y_k) = (x_1 - (2k-1), x_2 - (2k-3), \dots, x_{k-1} - 3, x_k - 1)$. Thus, the problem is reduced into counting the number of partitions that have at most k parts. The generating function of partitions with at most k parts is precisely $\frac{1}{(q;q)_k}$.

But notice that $1 + 3 + 5 + 7 + \cdots + (2k-1) = k^2$, so we need to multiply q^{k^2} back to add back the k^2 objects we initially removed. Thus we conclude that the left-hand side signifies the generating function of partitions whose consecutive parts differ by at least 2.

We will now prove that

$$G_1(1;q) = 1 + \sum_{n=1}^{\infty} \frac{q^{k^2}}{(q;q)_k}.$$

Suppose that the $B(n;q)$ satisfy

$$G_1(z;q) = \sum_{n=0}^{\infty} B(n;q) z^n.$$

But thanks to (1) and (3) of Lemma 5.1, we have $G_1(z;q) = G_0(z;q) + zqG_0(zq;q) = G_1(zq;q) + zqG_1(zq^2;q)$. Hence it follows that

$$\sum_{n=0}^{\infty} B(n;q) z^n = \sum_{n=0}^{\infty} B(n;q) q^n z^n + \sum_{n=0}^{\infty} B(n;q) q^{2n+1} z^{n+1},$$

so comparing the coefficients gives us $B(n;q) = B(n;q)q^n + B(n-1;q)q^{2n-1}$. Also, note that $G_1(0;q) = B(0;q) = 1$. Repeated applications of this recurrence relation gives us

$$\begin{aligned} B(n;q) &= \frac{q^{2n-1}}{1-q^n} B(n-1;q) = \frac{q^{2n-1}}{1-q^n}\frac{q^{2n-3}}{1-q^{n-1}} B(n-2;q) \\ &= \frac{q^{2n-1}}{1-q^n}\frac{q^{2n-3}}{1-q^{n-1}}\frac{q^{2n-5}}{1-q^{n-2}} B(n-3;q) \\ &= \cdots = \frac{q^{(2n-1)+(2n-3)+\cdots+1}}{(q;q)_n} B(0;q) = \frac{q^{n^2}}{(q;q)_n}. \end{aligned}$$

Hence, we indeed have, upon letting $z = 1$,

$$G_1(1;q) = 1 + \sum_{k=1}^{\infty} \frac{q^{k^2}}{(q;q)_k}.$$

On the other hand, notice that (with $\overset{\dagger\dagger}{=}$ marking where n is replaced by $-n-1$)

$$\begin{aligned}
G_1(1;q) &= \frac{1}{(q;q)_\infty}\sum_{n=0}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+1)}(1-q^{4n+2}) \\
&= \frac{1}{(q;q)_\infty}\left(\sum_{n=0}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+1)} - \sum_{n=0}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+9)+2}\right) \\
&\overset{\dagger\dagger}{=} \frac{1}{(q;q)_\infty}\left(\sum_{n=0}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+1)} - \sum_{n=-\infty}^{-1}(-1)^{-n-1} q^{\frac{1}{2}(-n-1)(-5n+4)+2}\right) \\
&= \frac{1}{(q;q)_\infty}\left(\sum_{n=0}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+1)} + \sum_{n=-\infty}^{-1}(-1)^n q^{\frac{1}{2}n(5n+1)}\right) \\
&= \frac{1}{(q;q)_\infty}\sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+1)} = \frac{1}{(q;q)_\infty}\sum_{n=-\infty}^{\infty}(q^{\frac{5}{2}})^{n^2}(-q^{\frac{1}{2}})^n.
\end{aligned}$$

Applying Theorem 3.4 thus gives us

$$\begin{aligned}
G_1(1;q) &= \frac{1}{(q;q)_\infty}((q^{\frac{5}{2}})^2;(q^{\frac{5}{2}})^2)_\infty(-(-q^{\frac{1}{2}}q^{\frac{5}{2}});(q^{\frac{5}{2}})^2)_\infty(-(-q^{-\frac{1}{2}}q^{\frac{5}{2}});(q^{\frac{5}{2}})^2)_\infty \\
&= \frac{(q^5;q^5)_\infty(q^3;q^5)_\infty(q^2;q^5)_\infty}{(q;q)_\infty} = \frac{(q^5;q^5)_\infty(q^3;q^5)_\infty(q^2;q^5)_\infty}{(q,q^2,q^3,q^4,q^5;q^5)_\infty} = \frac{1}{(q,q^4;q^5)_\infty},
\end{aligned}$$

so, as required,

$$1+\sum_{k=1}^{\infty}\frac{q^{k^2}}{(q;q)_k} = G_1(1;q) = \frac{1}{(q,q^4;q^5)_\infty} = \prod_{k=0}^{\infty}\frac{1}{(1-q^{5k+1})(1-q^{5k+4})}. \qquad \square$$

Proof of Rogers-Ramanujan II. Start with the left-hand side. Suppose that $(x_1,\ldots,x_k)$ (as always, assume $x_1 \geq x_2 \geq \cdots \geq x_k$) is a partition whose difference between two consecutive parts is at least 2 and whose smallest part is at least 2. Since $x_k \geq 2$, it follows that there is a set of non-negative integers $(y_1,\ldots,y_k)$ such that $(y_1,\ldots,y_k) = (x_1-2k, x_2-(2k-2),\ldots,x_{k-1}-4, x_k-2)$. Thus, the problem is reduced into counting the number of partitions that have at most k parts. The generating function of partitions with at most k parts is precisely $\frac{1}{(q;q)_k}$.

But notice that $2+4+6+8+\cdots+2k = 2(1+2+\cdots+k) = k(k+1) = k^2+k$, so we need to multiply q^{k^2+k} back to add back the k^2+k objects we initially removed. Thus we can conclude that the left-hand side signifies the generating function of partitions whose consecutive parts differ by at least 2 and whose smallest part is at least 2.

We showed in the proof of Rogers-Ramanujan I that

$$G_1(z;q) = 1+\sum_{k=1}^{\infty}\frac{q^{k^2}z^k}{(q;q)_k}.$$

So upon plugging in $z=q$, we have

$$G_1(q;q) = 1+\sum_{n=1}^{\infty}\frac{q^{k^2+k}}{(q;q)_k}.$$

By Lemma 5.1(3), we have $G_1(q;q) = G_0(1;q)$. So it follows that (with $\overset{\dagger\dagger}{=}$ marking where n is replaced by $-n-1$)

$$\begin{aligned}
G_0(1;q) &= \frac{1}{(q;q)_\infty} \sum_{n=0}^{\infty} (-1)^n q^{\frac{1}{2}n(5n+3)}(1-q^{2n+1}) \\
&= \frac{1}{(q;q)_\infty} \left(\sum_{n=0}^{\infty} (-1)^n q^{\frac{1}{2}n(5n+3)} - \sum_{n=0}^{\infty} (-1)^n q^{\frac{1}{2}n(5n+7)+1} \right) \\
&\overset{\dagger\dagger}{=} \frac{1}{(q;q)_\infty} \left(\sum_{n=0}^{\infty} (-1)^n q^{\frac{1}{2}n(5n+1)} - \sum_{n=-\infty}^{-1} (-1)^{-n-1} q^{\frac{1}{2}(-n-1)(-5n+2)+1} \right) \\
&= \frac{1}{(q;q)_\infty} \left(\sum_{n=0}^{\infty} (-1)^n q^{\frac{1}{2}n(5n+3)} + \sum_{n=-\infty}^{-1} (-1)^n q^{\frac{1}{2}n(5n+3)} \right) \\
&= \frac{1}{(q;q)_\infty} \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{1}{2}n(5n+3)} = \frac{1}{(q;q)_\infty} \sum_{n=-\infty}^{\infty} (q^{\frac{5}{2}})^{n^2} (-q^{\frac{3}{2}})^n .
\end{aligned}$$

Applying Theorem 3.4 thus gives us

$$\begin{aligned}
G_0(1;q) &= \frac{1}{(q;q)_\infty}((q^{\frac{5}{2}})^2;(q^{\frac{5}{2}})^2)_\infty(-(-q^{\frac{3}{2}}q^{\frac{5}{2}});(q^{\frac{5}{2}})^2)_\infty(-(-q^{-\frac{3}{2}}q^{\frac{5}{2}});(q^{\frac{5}{2}})^2)_\infty \\
&= \frac{(q^5;q^5)_\infty(q^4;q^5)_\infty(q;q^5)_\infty}{(q;q)_\infty} = \frac{(q^5;q^5)_\infty(q^4;q^5)_\infty(q;q^5)_\infty}{(q,q^2,q^3,q^4,q^5;q^5)_\infty} = \frac{1}{(q^2,q^3;q^5)_\infty},
\end{aligned}$$

so, as required,

$$1 + \sum_{k=1}^{\infty} \frac{q^{k^2+k}}{(q;q)_k} = G_1(q;q) = G_0(1;q) = \frac{1}{(q,q^2;q^3)_\infty} = \prod_{k=0}^{\infty} \frac{1}{(1-q^{5k+2})(1-q^{5k+3})}. \qquad \square$$

A different proof of Rogers–Ramanujan involving the Ramanujan integral will be given in the analysis portion of this lecture.

6. Finite fields

6.1. **Vector space counting**

Definition 6.1. A *field* F is a commutative ring with identity such that every non-zero element has a (unique) multiplicative inverse. In particular, if there are finitely many elements, then F is said to be a *finite field.* A finite field with q elements is denoted by $\mathbb{F}_q$.

Example. Let $\mathbb{Z}/7\mathbb{Z} = \{0,1,2,3,4,5,6\}$, and let the addition (resp. multiplication) defined by addition (resp. multiplication) followed by reducing modulo 7. These two operations indeed form a commutative ring with unity 1, so we only need to verify if every non-zero element has a multiplicative inverse. Since $\gcd(a,7) = 1$ for all non-zero elements in $\mathbb{Z}/7\mathbb{Z}$, it follows that every non-zero element has a multiplicative inverse. This argument holds fro any prime, so $\mathbb{Z}/p\mathbb{Z}$ is a field for any p. Such is also an example of a finite field.

Let $V_n(q)$ be an n-dimensional vector space over $\mathbb{F}_q$. Clearly, $V_n(q)$ must have q^n vectors (hence, $V_n(q) = \mathbb{F}_{q^n}$). We are interested in counting the number of k linear independent vectors in $V_n(q)$, which is important in counting how many k-dimensional subspaces of $V_n(q)$ there are.

For the first vector, we can choose any vector except for the zero vector, so we have $(q^n - 1)$ options. After that, we can choose any vector except for the vector in the subspace generated by the initially chosen vector; thus, there are $(q^n - q)$ options. There are q^2 vectors in the subspace generated by the two chosen vectors; thus, for the third vector there are $(q^n - q^2)$ options to choose from. Continuing on, we have

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}).$$

Does this correspond to the number of k-dimensional subspaces of $V_n(q)$? Certainly not because we are over-counting the number of k linear independent sets: we are counting any identical linearly independent subset whose vectors appear in different orders as distinct sets. To account for this, we need to divide by $(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$. Thus, there are

$$\frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} = \begin{bmatrix} n \\ k \end{bmatrix}_q$$

subsets of k linear independent vectors in $V_n(q)$. Therefore, we have proved the following theorem.

Theorem 6.1. *The number of k-dimensional subspaces of $V_n(q)$ is* $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

6.2. Connection to partitions and the finite q-binomial theorem

As an example, consider a 9-dimensional space. Suppose that the row reduced echelon form of a 3×9 matrix is as follows.

$$\begin{pmatrix} 0 & 1 & * & * & 0 & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 1 & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * \end{pmatrix}$$

Since there are three linearly independent columns, it follows that the row vectors from the original matrix generates a three-dimensional subspace.

Now, suppose that each $*$ is an element of a finite field $\mathbb{F}_q$. We claim that every matrix of such form corresponds to a partition that fit in a 3×6 box. Note that the $*$'s form the right justified Ferrers diagram. Note that any row, in this case, can have up to six entries that need not be 0 or 1. Thus, the number of a 3×9 reduced row echolon forms with three 1s is equal to the number of partitions that fit in a 3×6 box. Hence, there are $\begin{bmatrix} 9 \\ 3 \end{bmatrix}_q$ partitions.

Theorem 6.2. *There are*

$$\begin{bmatrix} n \\ n-k \end{bmatrix}_q \begin{bmatrix} m \\ k \end{bmatrix}_q (q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$$

$m \times n$ matrices of rank k with entries from $\mathbb{F}_q$.

Proof. Consider a linear transformation $T : V_n(q) \to V_m(q)$ such that $\dim(T(V_n(q))) = k$. By the rank-nullity theorem, the nullity of T must be an $(n-k)$-dimensional subspace. Indeed, there are $\begin{bmatrix} n \\ n-k \end{bmatrix}_q$ subspaces for the null space. Similarly, there are $\begin{bmatrix} m \\ k \end{bmatrix}_q$ subspaces for the range of T. Finally, note that within the same null space and the same range, there are $(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})$ distinct linear transformations. □

Corollary 6.1. $\displaystyle\sum_{k=0}^{\min(m,n)} \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} m \\ k \end{bmatrix}_q (q^k-1)\cdots(q^k-q^{k-1}) = q^{mn}.$

Proof. Clearly there are q^{mn} $m\times n$ matrices. Any $m\times n$ matrix can have rank 0 up to $\min(m,n)$. Thus summing up the total number of matrices of each rank gives us the total number of possible $m\times n$ matrices. □

Note that

$$\begin{aligned}\begin{bmatrix} m \\ k \end{bmatrix}_q (q^k-1)\cdots(q^k-q^{k-1}) &= (-1)^k q^{k(k-1)/2}\frac{(q;q)_m(1-q)(1-q^2)\cdots(1-q^k)}{(q;q)_k(q;q)_{m-k}} \\ &= (-1)^k q^{\binom{k}{2}}\frac{(q;q)_m}{(q;q)_{m-k}} = (-1)^k q^{\binom{k}{2}}(1-q^m)\cdots(1-q^{m-k+1}).\end{aligned}$$

This gives us another way of writing Corollary 6.1.

Corollary 6.2. $q^{mn} = \displaystyle\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (-1)^k q^{\binom{k}{2}}(1-q^m)\cdots(1-q^{m-k+1}).$

Now replacing q^m with x gives us

Theorem 6.3. $x^n = \displaystyle\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (-1)^k q^{\binom{k}{2}} \prod_{j=0}^{k-1}(1-xq^{-j}) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q \prod_{j=0}^{k-1}(x-q^j).$

Remark. Note that both sides of the above theorem are analytic in x.

We claim that Theorem is the q-binomial theorem. To see why, let's juxtapose this theorem with the original q-binomial theorem we proved, namely

$$(1-x)(1-xq)\cdots(1-xq^{n-1}) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (-1)^k q^{\binom{k}{2}} x^k.$$

Expanding the LHS gives us

$$(1-x)(1-xq)\cdots(1-xq^{n-1}) = x^n\left(\frac{1}{x}-1\right)\cdots\left(\frac{1}{x}-q^{n-1}\right).$$

Now perform the change of variables by letting $x := y^{-1}$. Then we have

$$x^n\left(\frac{1}{x}-1\right)\cdots\left(\frac{1}{x}-q^{n-1}\right) = y^{-n}\prod_{j=0}^{n-1}(y-q^j) = \sum_{n=0}^{k} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{k}{2}}(-1)^k y^{-k} y^n.$$

Now multiplying both sides by y^n gives us, and then just switching back to x gives us

$$\prod_{j=0}^{n-1}(x-q^j) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (-1)^{n-k} q^{\binom{n-k}{2}} x^k.$$

Thus in essence, the operation is a change of basis from $\{1, x, x^2, \dots\}$ to $\{(x;q)_n\}_{n\in\mathbb{N}\cup\{0\}}$. We only showed that such change of basis procedure can be done between the two aforementioned particular bases. However, we can carry out this operation in general through the Vandermonde inversion.

Theorem 6.4 (Vandermonde inversion)**.**

$$b_n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q a_k$$

if and only if

$$a_n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (-1)^{n-k} q^{\binom{n-k}{2}} b_k.$$

Proof. Note that

$$\begin{aligned} \sum_{n=0}^{\infty} \frac{b_n}{(q;q)_n} t^n &= \sum_{n=0}^{\infty} \frac{t_n}{(q;q)_n} \sum_{k=0}^{n} \frac{(q;q)_n}{(q;q)_k (q;q)_{n-k}} a_k \\ &= \sum_{k=0}^{\infty} \frac{a_k}{(q;q)_k} \sum_{n=k}^{\infty} \frac{t^n}{(q;q)_{n-k}}. \end{aligned}$$

Changing the variable $n \to m + k$ gives us

$$\sum_{k=0}^{\infty} \frac{a_k}{(q;q)_k} \sum_{n=k}^{\infty} \frac{t^n}{(q;q)_{n-k}} = \sum_{k=0}^{\infty} \frac{a_k t^k}{(q;q)_k} \sum_{m=0}^{\infty} \frac{t^m}{(q;q)_m} = \frac{1}{(t;q)_\infty} \sum_{k=0}^{\infty} \frac{a^k t^k}{(q;q)_k}.$$

Thus, by the (infinite) q-binomial theorem,

$$\sum_{k=0}^{\infty} \frac{a_k t^k}{(q;q)_k} = (t;q)_\infty \sum_{k=0}^{\infty} \frac{t^k b_k}{(q;q)_k} = \sum_{k,j=0}^{\infty} \frac{(-1)^j}{(q;q)_j} q^{\binom{j}{2}} t^j \frac{t^k b_k}{(q;q)_k}.$$

Hence

$$\frac{a_n}{(q;q)_n} = \sum_{k=0}^{n} \frac{(-1)^{n-k} q^{\binom{n-k}{2}}}{(q;q)_k (q;q)_{n-k}} b_k.$$

Note that the whole process is reversible, so the reverse direction can be shown similarly. □

7. Rogers–Szegő polynomials and q-Hermite polynomials

Definition 7.1. The *Rogers–Szegő polynomial* $h_n(x;q)$ is given by

$$h_n(x;q) := \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q x^k$$

The alternative form called the *(continuous) q-Hermite polynomial* is

$$H_n(x \,|\, q) := \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q e^{i(n-2k)\theta}.$$

We claim that $H_n(x\,|\,q)$ is a polynomial in $x = \cos\theta$. By the symmetry of the q-binomial coefficients, we see that the terms $e^{i(n-2k)\theta}$ and $e^{i(n-2(n-k))\theta} = e^{i(-n+2k)\theta}$ have the same coefficient. But then note that

$$e^{i(n-2k)\theta} + e^{i(-n+2k)\theta} = 2\cos(n-2k)\theta,$$

so indeed the q-Hermite polynomials are polynomials in $\cos\theta$. q-Hermite polynomials will be covered more in depth in the analysis lecture note, so we will focus more on the Rogers–Szegő polynomials.

Theorem 7.1. *The Rogers–Szegő polynomials satisfy the following linearization formula*

$$h_n(x;q)h_m(x;q) = \sum_{k=0}^{\min(m,n)} \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} m \\ k \end{bmatrix}_q (q;q)_k x^k h_{m+n-2k}(x;q).$$

The inverse formula of $h_n(x;q)$ is

$$h_{m+n}(x;q) = \sum_{k=0}^{\min(m,n)} \begin{bmatrix} m \\ k \end{bmatrix}_q \begin{bmatrix} n \\ k \end{bmatrix}_q (q;q)_k q^{\binom{k}{2}} (-x)^k h_{m-k}(x;q) h_{n-k}(x;q).$$

The q-Hermite counterpart will be stated and proved in the analysis lecture note.

Proof. We will prove the inverse formula, since the linearization follows from the inverse. The LHS is the generating function of all subspaces of $V_{m+n}(q) = V_n(q) \oplus V_m(q)$. If W is a t-dimensional subspace of $V_{m_n}(q)$, then $W \cong W_1 \oplus W_2 \oplus W_3$, where $W_1 = W \cap V_n(q)$ is an s-dimensional space, $W_2 = W \cap V_m(q)$ is a u-dimensional space, and W_3 is a v-dimensional subspace of $V_n(q)/W_1 \oplus V_m(q)/W_2$ such that $W_3 \cap (V_n(q)/W_1) = W_3 \cap (V_m(q)/W_2) = \{0\}$. Note we want to have $s + u + t = v$.

Now count how many subspaces there are, for each of W_i. There are $\begin{bmatrix} n \\ s \end{bmatrix}_q$ subspaces available for W_1, and $\begin{bmatrix} m \\ u \end{bmatrix}_q$ subspaces available for W_2. As for the last type, it's equivalent to computing the number of matrices of dimension $(n-s) \times (m-u)$ with rank v, so we have

$$\begin{bmatrix} n-s \\ n-s-v \end{bmatrix}_q \begin{bmatrix} m-u \\ v \end{bmatrix}_q (q^v - 1) \cdots (q^v - q^{v-1}),$$

so we have

$$\begin{bmatrix} m+n \\ t \end{bmatrix}_q = \sum_{s+u+v=t} \begin{bmatrix} n \\ s \end{bmatrix}_q \begin{bmatrix} m \\ u \end{bmatrix}_q \begin{bmatrix} n-s \\ v \end{bmatrix}_q \begin{bmatrix} m-u \\ v \end{bmatrix}_q \prod_{j=0}^{v-1} (q^v - q^j).$$

So the generating function $h_{m+n}(x;q)$ is

$$\begin{aligned} h_{m+n}(x;q) &= \sum_{t=0}^{m+n} \begin{bmatrix} m+n \\ t \end{bmatrix}_q x^t \\ &= \sum_{v=0}^{\min(m,n)} \begin{bmatrix} n \\ v \end{bmatrix}_q \begin{bmatrix} m \\ v \end{bmatrix}_q \left(\prod_{j=0}^{v-1} (q^v - q^j) \right) x^v \sum_{s=0}^{n-v} \begin{bmatrix} n-v \\ s \end{bmatrix}_q x^s \sum_{u=0}^{m-v} \begin{bmatrix} m-v \\ u \end{bmatrix}_q x^u \end{aligned}$$

$$= \sum_{v=0}^{\min(m,n)} \begin{bmatrix} n \\ v \end{bmatrix}_q \begin{bmatrix} m \\ v \end{bmatrix}_q \prod_{j=0}^{v-1} (q^v - q^j) x^v h_{n-v}(x;q) h_{m-v}(x;q),$$

so the inverse formula follows upon observing that

$$\prod_{j=0}^{v-1} q^v - q^j = \prod_{j=0}^{v-1} (-1) q^j (1 - q^{v-j}) = (-1)^v q^{0+\cdots+(v-1)} (q;q)_v = (-1)^v q^{\binom{v}{2}} (q;q)_v. \qquad \square$$

7.1. **Interlude: Perfect matching**

We provide one interesting combinatorial application of the q-Hermite polynomials. Since the proofs are beyond the scope of this course, we will just state some interesting results. An interesting reader, for instance, can learn more about the concepts in this section from Ismail, Stanton, and Viennot [ISV87].

Definition 7.2. Let $\{S_1, \dots, S_k\}$ be a multiset of numbers such that $|S_i| = n_i$ for all $1 \le i \le k$. Suppose that $x \in S_i$ and $y \in S_j$ with $i < j$ implies $x < y$, and arrange these real numbers in a real line. A *perfect matching* is a pairing $(x, \alpha(x))$ of the elements of $\bigcup S_j$ such that:

(1) $\alpha(x) \notin S_j$ if $x \in S_j$, and
(2) $\alpha(x) \neq \alpha(y) \Leftrightarrow x \neq y$.

Then $(x, \alpha(x))$ is an *edge* of α. If $x < y < \alpha(x), \alpha(y)$, then we say that the edges $(x, \alpha(x)), (y, \alpha(y))$ *produce a crossing.* Finally, the crossing number, denoted $\operatorname{cr}(\alpha)$, is the number of crossings generated by the edges in α.

We state one property of the H_n's without stating the proof.

Proposition 7.1. $\int_{-\infty}^{\infty} w(x;q) H_m(x \mid q) H_n(x \mid q) = 0$ *if* $m \neq n$*, where* w *is the weight function defined by*

$$w(x;q) := \frac{\prod_{n=0}^{\infty} (1 - 2(2x^2-1)q^n + q^{2n})}{\sqrt{1-x^2}}.$$

Theorem 7.2. *We have, for an appropriate weight function* $w(x;q)$*,*

$$\int_{-\infty}^{\infty} w(x;q) H_{n_1}(x \,|\, q) \cdots H_{n_k}(x \,|\, q)\, dx = c(n_1, \dots, n_k; q).$$

The constant $c(n_1, \dots, n_k; q)$ *is equal to*

$$c(n_1, \dots, n_k; q) := \sum_{\alpha} q^{\operatorname{cr}(\alpha)},$$

summed over all the available perfect matchings of $n = n_1 + \cdots + n_k$ *numbers partitioned into* $n_1, \dots, n_k$ *elements.*

8. Möbius inversion formula

We will first start with the most familiar version of Möbius inversion.

8.1. **Number-theoretic Möbius inversion formula**

We first start with a fundamental result that one sees in elementary number theory but nonetheless important.

Theorem 8.1 (Fundamental theorem of arithmetic)**.** *Any $n \in \mathbb{N}$ has a unique factorization, i.e., there are primes $p_1, \dots, p_k$ and $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ such that $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, and such factorization is unique up to order.*

Definition 8.1. We say any function $f : \mathbb{N} \to \mathbb{C}$ is an *arithmetical function* (or an *arithmetic function*). Particularly,

(1) if $f(a+b) = f(a) + f(b)$ for all $\gcd(a, b) = 1$, then f is said to be *additive.* If the coprime condition can be removed, then f is said to be *completely additive.*

(2) if $f(ab) = f(a)f(b)$ for all $\gcd(a, b) = 1$ and is not identically zero, then f is said to be *multiplicative.* If the coprime condition can be removed, then f is said to be *completely multiplicative.*

Definition 8.2. The *Möbius function* $\mu : \mathbb{N} \to \mathbb{Z}$ is an arithmetical function defined by

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ is squarefree with } k \text{ prime factors;} \\ 0 & \text{otherwise.} \end{cases}$$

Definition 8.3. The *Riemann zeta function* $\zeta(s)$ is defined as

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s},$$

for all $\mathrm{R}e(s) > 1$.

Theorem 8.2. $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s} = \left[\prod_{j=1}^{\infty} \left(1 - \frac{1}{p_j^s}\right)\right]^{-1}.$

Proof. We are essentially performing the Eratosthenes sieve here. Since

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \cdots,$$

it follows that

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \cdots$$

Continuing this operation for $3, 5, 7$, and so forth, we have

$$\prod_{j=1}^{\infty} \left(1 - \frac{1}{p_j^s}\right)\zeta(s) = 1, \text{ so } \zeta(s) = \left[\prod_{j=1}^{\infty} \left(1 - \frac{1}{p_j^s}\right)\right]^{-1}.$$

Finally, notice that the infinite product converges if and only if $\mathrm{R}e(s) > 1$, so the claim follows. □

Lemma 8.1. *$\prod(1 + a_n)$ converges if and only if $\sum |a_n|$ converges.*

Therefore, $\prod(1 - p_j^{-s})$ converges if and only if $\sum p_j^{-s}$ converges, and this happens if and only if $\mathrm{R}e(s) > 1$.

Definition 8.4. A *Dirichlet series* is a series of the form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where $a_n, s \in \mathbb{C}$.

Theorem 8.3. *The Dirichlet series of* $\mu(n)$ *is*

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{j=1}^{\infty} \left(1 - \frac{1}{p_j^s}\right) = \frac{1}{\zeta(s)}.$$

Therefore,

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1.$$

Proof. Notice that

$$1 = \left(\sum_{m=1}^{\infty} \frac{1}{m^s}\right) \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) = \sum_{m,n=1}^{\infty} \frac{\mu(n)}{m^s n^s} = \sum_{n=1}^{\infty} \frac{\mu(n)}{(mn)^s} = \sum_{N=1}^{\infty} \frac{1}{N^s} \sum_{n|N} \mu(n),$$

upon letting $mn =: N$. Therefore, we see that

$$\sum_{n|N} \mu(N) = \delta_{N,1},$$

so the theorem follows. □

Theorem 8.4 (Möbius inversion formula)**.** *Let* f *and* g *be arithmetical functions. Then*

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right).$$

Proof. Suppose that

$$f(n) = \sum_{d|n} g(d).$$

Then

$$\begin{aligned} \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{d_1|d} g(d_1) = \sum_{dk=n} \mu(k) \sum_{d_1 d_2 = d} g(d_1) \\ &= \sum_{dk=n} \sum_{d_1 d_2 = d} \mu(k) g(d_1) = \sum_{d_1 d_2 k = n} \mu(k) g(d_1) \\ &= \sum_{d_1 d_2 k = n} g(d_1) \sum_{k|\frac{n}{d_1}} \mu(k). \end{aligned}$$

But recall that $\sum_{k|m} \mu(k) = 0$ if and only if $m = 1$. Thus the second sum vanishes if and only if $n \neq d_1$. Therefore

$$\sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) = g(n).$$

□

8.2. **Partially ordered sets and incidence algebra**

Definition 8.5. A set $(S, \leq)$ is a *partially ordered set* (or *poset*) if $\leq$ is

1. reflexive ($a \leq a$ fo all $a \in S$),
2. anti-symmetric ($a \leq b$ and $b \leq a$ implies $a = b$ for all $a, b \in S$), and
3. transitive ($a \leq b$ and $b \leq c$ imply $a \leq c$ for all $a, b, c \in S$).

Definition 8.6. We say $a, b \in S$ are comparable if $a \leq b$ or $b \leq a$. In this case, we will denote $a \vee b$ the larger of the two, and $a \wedge b$ the smaller of the two.

Definition 8.7. If $(S, \leq)$ is a partially ordered set such that every two elements has a unique supremum and a unique infimum is said to be a *lattice*.

Definition 8.8. We denote $[x, y] := \{z : x \leq z \leq y\} \subseteq S$. If $[x, y]$ is finite, then S is said to be *locally finite*.

We will assume throughout this course that partially ordered sets are locally finite.

Definition 8.9. For any P and Q two partially ordered sets, we shall denote $\mathrm{Hom}(P, Q)$ the set of all monotone function $f : P \to Q$, i.e., $x \leq y \Rightarrow f(x) \leq f(y)$.

Definition 8.10. Let P be a partially ordered set. The *incidence algebra* of P – denoted $\mathrm{ia}(P)$ – is the set of functions mapping an interval to a field, i.e., for any $x, y \in P$ such that $x \leq y$, there is $k \in K$ such that $f(x, y) = f([x, y]) = k$, where K is some field. For any $x \not\leq y$, we define $f(x, y) = 0$.

For $\mathrm{ia}(P)$, scalar multiplication and addition are defined as usual pointwise scalar multiplication and addition, as usual. Multiplication $*$ is defined by the following convolution for any $x \leq y$:

$$(f * g)(x, y) := \sum_{x \leq z \leq y} f(x, z) g(z, y).$$

This naturally leads to define the multiplicative identity element of the incidence algebra.

Definition 8.11. The multiplicative identity element of an incidence algebra (i.e., $\delta * f = f * \delta = f$ for all $f \in \mathrm{ia}(P)$) is called the *(Kronecker) δ function* which is defined by

$$\delta(x, y) := \begin{cases} 1 & (x = y) \\ 0 & (x \neq y). \end{cases}$$

To see why δ is the multiplicative identity, note that

$$\begin{aligned}(f \circ \delta)(x, y) &= \sum_{x \leq z \leq y} f(x, z)\delta(z, y) = f(x, y)\delta(y, y) + \sum_{x \leq z < y} f(x, z)\delta(z, y) \\ &= f(x, y) + \sum_{x \leq z < y} f(x, z) \cdot 0 = f(x, y).\end{aligned}$$

Definition 8.12. The *ζ function* of an incidence algebra (distinct from the Riemann zeta function) is defined by

$$\zeta(x, y) := \begin{cases} 1 & (x \leq y) \\ 0 & (x \not\leq y). \end{cases}$$

In fact, the multiplication as defined in ia(P) gives rise to an algebra over a field, which justifies the naming incidence *algebra*. Since the verification of the necessary axioms is straightforward, we will recall the definition of algebra, state this claim formally, and omit the proof.

Definition 8.13. Let K be a field. Then A is an *algebra over K* (or *K-algebra*) if A is a vector space with the multiplication operation satisfying bilinearity, i.e., for all $x, y, z \in A$ and scalars $a, b \in K$,

(1) $(x + y) \cdot z = x \cdot z + y \cdot z$
(2) $x \cdot (y + z) = x \cdot y + x \cdot z$
(3) $(ax) \cdot (by) = (ab)(x \cdot y)$.

Theorem 8.5. *For a partially ordered set P and a field K, ia(P) is a K-algebra.*

Also, before defining the Möbius function for incidence algebras, we are required to ascertain the existence of an inverse.

Proposition 8.1. *Let $f \in$ ia(P) for a locally finite poset P, and $*$ be the convolution operation.*

(1) $*$ is associative.
(2) $*$ is both left- and right-distributive (with respect to scalar multiplication and addition).
(3) f has an inverse if and only if $f(x, x) \neq 0$ for any $x \in P$.

Proof. (1) We have

$$(f * g) * h(x, y) = \sum_{x \leq z \leq y} (f * g)(x, z)h(z, y) = \sum_{x \leq z \leq y} \sum_{x \leq w \leq z} f(x, w)g(w, z)h(z, y)$$
$$= \sum_{x \leq w \leq y} f(x, w) \sum_{w \leq z \leq y} g(w, z)h(z, y) = \sum_{x \leq w \leq y} f(x, w)(g * h)(w, y) = f * (g * h).$$

(2) Since right-distributivity can be proved similarly, we will only cover the left-distributivity, where $a \in K$.

$$[f * (g + h)](x, y) = \sum_{x \leq z \leq y} f(x, z)[(g + h)(z, y)] = \sum_{x \leq z \leq y} f(x, z)[g(z, y) + h(z, y)]$$
$$= \sum_{x \leq z \leq y} f(x, z)g(z, y) + \sum_{x \leq z \leq y} f(x, z)h(z, y) = f * g + f * h.$$
$$[f * (ag)](x, y) = \sum_{x \leq z \leq y} f(x, z)[(ag)(z, y)] = \sum_{x \leq z \leq y} f(x, z)ag(z, y)$$
$$= \sum_{x \leq z \leq y} a(f(x, z)g(z, y)) = a \sum_{x \leq z \leq y} f(x, z)g(z, y) = a(f * g).$$

(3) First we will assume that f has a left inverse f_L^{-1} and a right inverse f_R^{-1}, and show that they must be equal, which justifies calling such function the "inverse" of f. We have $f_L^{-1} \circ f = \delta$ and $f * f_R^{-1} = \delta$, so

$$f_L^{-1} = f_L^{-1} * \delta = f_L^{-1} * (f * f_R^{-1}) = (f_L^{-1} * f) * f_R^{-1} = f_R^{-1},$$

from which it follows $f_L^{-1} = f_R^{-1} =: f^{-1}$. Thus it suffices to ascertain the existence of f_L^{-1} and f_R^{-1}. Again, since proving the existence of f_L^{-1} works similarly with that of the right counterpart, we will only prove the existence of f_R^{-1} here. Note that f_R^{-1} must satisfy

$$\sum_{x \le z \le y} f(x,z) f_R^{-1}(z,y) = \delta(x,y). \tag{8.1}$$

If $x = y$, then we must have $f(x,x)f_R^{-1}(x,x) = 1$. Therefore $f_R^{-1}(x,x) = (f(x,x))^{-1}$ is well-defined if and only if $f(x,x) \neq 0$ for any $x \in P$. Using the fact that $f_R^{-1}(x,x) = 1/f(x,x)$ and (8.1), we can recursively define $f_R^{-1}(x,y)$ where $[x,y]$ contains more than one element.

Suppose that one defined the values of $f_R^{-1}(x,y)$ where $[x,y]$ contains at most n elements. Now if $[x,y]$ has cardinality $n+1$, we have by (8.1) that

$$f(x,x)f_R^{-1}(x,y) + \sum_{x < z \le y} f(x,z)f_R^{-1}(z,y) = 0.$$

Note that $f_R^{-1}(z,y)$ is defined since $[z,y]$ has at most n elements for any $x < z \le y$, thereby completing the proof. □

Now that we established that any function with $f(x,x) \neq 0$ has an inverse, we are now certain that the Möbius function, as defined below, exists for any incidence algebra.

Definition 8.14. The *Möbius function* of an incidence algebra is the inverse of ζ, i.e., $\mu * \zeta = \delta$.

Remark. One can also consider the incidence algebra over the product of two posets P and Q (i.e., $P \times Q$), with partial order defined by $(p,q) \le (p',q')$ if and only if $p \le_P p'$ and $q \le_Q q'$. In this case, if f is in the incidence algebra of $P \times Q$ (suppose $f : P \times Q \to \mathbb{R}$), then we must have $f((p,q),(p',q')) = 0$ provided either $p \not\le_P p'$ or $q \not\le_Q q'$.

Remark. Since $\mu(x,y)$ is the inverse of ζ, it follows that we must have

$$\sum_{x \le z \le y} \mu(x,z) = \sum_{x \le z \le y} \mu(z,y) = 0,$$

provided $x \neq y$. Thus it follows that

$$\mu(x,y) = -\sum_{x \le z < y} \mu(x,z).$$

Furthermore $\mu(x,x) = 1$. Thus from the following conditions, we may derive the value of μ inductively.

8.3. Möbius inversion formula for partially ordered sets

The goal of this section is to formally state the Möbius inversion formula in the most general settings possible (i.e., for all partially ordered sets) and prove the formula.

Theorem 8.6 (Möbius inversion formula for posets)**.** *Let P be a locally finite poset, and μ the Möbius function for* ia(P)*, a K-algebra. Suppose that f and g are functions from P to K, and that P has a unique minimum element. Then*

$$g(y) = \sum_{x \le y} f(x) \textit{ if and only if } f(y) = \sum_{x \le y} g(x)\mu(x,y).$$

If P has a unique maximum element, then we also have

$$g(y) = \sum_{x \geq y} f(x) \text{ if and only if } f(y) = \sum_{x \geq y} \mu(y,x) g(x).$$

Proof. Since the second part can be proved similarly, we will only prove the first part.

Since P is locally finite, all sums that appear in the theorem are finite. So for any y, we have

$$\begin{aligned} \sum_{x \leq y} g(x)\mu(x,y) &= \sum_{x \leq y} \left(\sum_{z \leq x} f(z) \right) \mu(x,y) = \sum_{z \leq y} \sum_{z \leq x \leq y} f(z)\mu(x,y) \\ &= \sum_{z \leq y} f(z) \sum_{z \leq x \leq y} \mu(x,y) = \sum_{z \leq y} f(z)\delta(z,x) = f(y). \end{aligned}$$

The reverse direction can be shown similarly.

$$\begin{aligned} \sum_{x \leq y} f(x) = \sum_{x \leq y} f(x)\zeta(x,y) &= \sum_{x \leq y} \left(\sum_{z \leq x} g(z)\mu(z,x) \right) \zeta(x,y) \\ &= \sum_{z \leq y} g(z) \sum_{z \leq x \leq y} \mu(z,x)\zeta(x,y) = \sum_{z \leq y} g(z)\delta(z,y) = g(y). \end{aligned}$$ □

Therefore, one can prove the number-theoretic Möbius inversion formula by defining $P = \mathbb{N}$ and letting $\leq$ be the divisibility relation. We shall introduce the q-analogue of the Möbius inversion formula in the next section.

9. Möbius functions in special settings

9.1. **Möbius function for boolean algebras**

Definition 9.1. A *boolean algebra* is a six-tuple $(A, \vee, \wedge, \neg, 0, 1)$ where:

1. 0 is the “least” element,
2. 1 is the “greatest” element,
3. $\neg$ denotes the “not” operation,
4. $\wedge$ is the“and” operation, and item $\vee$ is the “or” operation,

such that $\vee$ and $\wedge$ satisfy following conditions, for any $a, b, c \in A$:

1. (associativity) $(a \vee b) \vee c = a \vee (b \vee c), (a \wedge b) \wedge c = a \wedge (b \wedge c)$
2. (commutativity) $a \wedge b = b \wedge a, a \vee b = b \vee a$
3. (absorption) $a \wedge (a \vee b) = a \vee (a \wedge b) = a$
4. (identity) $a \vee 0 = a, a \wedge 0 = a$
5. (complement) $a \vee \neg a = 1, a \wedge \neg a = 0$
6. (distributivity) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c), a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Therefore, it follows that the set of all subsets of a set form a boolean algebra, where 0 is the empty set, 1 the entire set, $\vee = \cup$, $\wedge = \cap$, and $\neg$ the complement operation.

Now let’s calculate the Möbius function for boolean algebra. In fact, we claim that $\mu(X,Y) = (-1)^{|Y|-|X|}$, with the $\leq$ being the inclusion relation. Note that $\mu(X,X) = 1$ for any X. Thus, if $|Y| = 1 + |X|$, we have

$$\mu(X,Y) = - \sum_{X \leq Z < Y} \mu(X,Z) = -\mu(X,X) = -1.$$

If $|Y| = 2 + |X|$, then

$$\mu(X,Y) = -\sum_{X \leq Z < Y} \mu(X,Z) = -1 - (-2) = 1.$$

If $|Y| = 3 + |X|$, then

$$\begin{aligned}\mu(X,Y) = -\sum_{X \leq Z < Y} \mu(X,Z) &= -\left[1 + \binom{3}{1}(-1) + \binom{3}{2}(1)\right] \\ &= -(1 - 3 + 3) = -1.\end{aligned}$$

For the sake of induction, suppose that $\mu(X,Y) = (-1)^j$ for all $0 \leq j \leq n-1$. Note that if $|Y| = n + |X|$ and $X \leq Z < Y$, then $|Z| = j + |X|$ where $0 \leq j \leq n-1$, and there are $\binom{n}{j}$ possible subsets of Y. Thus we have, by the inductive hypothesis,

$$\mu(X,Y) = -\sum_{X \leq Z < Y} \mu(X,Z) = -\sum_{k=0}^{n-1} \binom{n}{k}(-1)^k.$$

But then recall that

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k,$$

so letting $x = -1$ gives that

$$\sum_{k=0}^{n} \binom{n}{k}(-1)^k = 0.$$

Hence, it follows that

$$\mu(X,Y) = -\sum_{X \leq Z < Y} \mu(X,Z) = -\sum_{k=0}^{n-1} \binom{n}{k}(-1)^k = (-1)^n,$$

completing the inductive step. Thus, as we will see in the proof of the next theorem, the inclusion-exclusion principle is a special case of Möbius inversion.

Theorem 9.1 (Inclusion-Exclusion principle). *If $A_1, \ldots, A_n \subseteq U$ with $|U| < \infty$, then*

$$\left|\bigcap_{j=1}^{n} A_j^c\right| = |U| + \sum_{k=1}^{n}(-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq n} |A_{i_1} \cap \cdots \cap A_{i_k}|.$$

Proof. Let P_i denote the property that $x \in A_i$. Thus, x satisfies the property P_i if and only if $x \in A_i$. Let B_n be the Boolean lattice on $\{1, 2, \ldots, n\}$. Then consider $E : B_n \to \mathbb{C}$ be the function defined by

$$E(I) := |\{x \in X : x \text{ satisfies } P_i \text{ for all } i \in I \textit{ and no others}\}|.$$

Similarly, let $L : B_n \to \mathbb{C}$ be the function defined by

$$L(I) := |\{x \in X : x \text{ satisfies } P_i \text{ for all } i \in I\}|.$$

Thus, unlike $E(I)$, $L(I)$ counts the number of elements that satisfy at least properties P_i for all $i \in I$ (and possibly others). For any $I \subseteq \{1, 2, \ldots, n\}$, therefore, we see that

$$L(I) = \left|\bigcap_{i \in I} A_i\right| = \sum_{I \subseteq J \subseteq \{1,2,\ldots n\}} E(J).$$

Hence the Möbius inversion formula gives us

$$E(I) = \sum_{I \subseteq J \subseteq \{1,2,\ldots,n\}} \mu(I,J)L(J) = \sum_{I \subseteq J \subseteq \{1,\ldots,n\}} (-1)^{|J|-|I|}L(J).$$

But then we want the size of the set $\bigcap_{j=1}^{n} A_j^c$, so we want to compute the number of elements in U that are not in any of $A_1, \ldots, A_n$, i.e., does not satisfy properties P_i for any $i \in \{1, 2, \ldots, n\}$. Thus letting $I = \emptyset$ yields

$$E(\emptyset) = \sum_{J \subseteq \{1,2,\ldots,n\}} (-1)^{|J|}L(J) = |U| + \sum_{k=1}^{n}(-1)^k \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=k}} \left|\bigcap_{i \in I} A_i\right|,$$

which is indeed the inclusion-exclusion principle we were looking for. □

9.2. Möbius function for the subspaces and the q-Möbius inversion formula

In this case, we say $X \leq Y$ if X is a subspace of Y, where X and Y are $\mathbb{F}_q$-vector spaces. If $\dim Y = \dim X$, then clearly $X = Y$. Thus $\mu(X, Y) = 1$. Suppose that $\dim Y = \dim X + 1$. Then we have

$$\mu(X, Y) = -\sum_{X \leq Z < Y} \mu(X, Z) = -1 = q^{\binom{1}{2}}(-1)^1,$$

since Z can only be X in this case. If $k := \dim Y - \dim X$ is equal to 2, then

$$\mu(X, Y) = -\sum_{X \leq Z < Y} \mu(X, Z) = -\left(1 - \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q\right) = -(1 - (1 + q)) = q = q^{\binom{2}{2}}(-1)^2.$$

If $k = 3$, then

$$\begin{aligned}\mu(X, Y) &= -\sum_{X \leq Z < Y} \mu(X, Z) = -\left(1 + \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q (-1) + \begin{bmatrix} 3 \\ 2 \end{bmatrix}_q q\right) \\ &= -[1 - (1 + q + q^2) + q(1 + q + q^2)] = -q^3 = q^{\binom{3}{2}}(-1)^3.\end{aligned}$$

Again, for the sake of induction, assume that that, for all $k \leq n - 1$, we have

$$\mu(X, Y) = -\sum_{X \leq Z < Y} \mu(X, Z) = q^{\binom{k}{2}}(-1)^k.$$

If $k = n$, then

$$\mu(X, Y) = -\sum_{X \leq Z < Y} \mu(X, Z) = -\left(\sum_{k=0}^{n-1} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{k}{2}}(-1)^k\right).$$

But by Theorem 3.1, we have

$$0 = (1;q)_n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{k}{2}} (-1)^k,$$

so it follows that

$$\mu(X,Y) = -\begin{bmatrix} n \\ n \end{bmatrix}_q q^{\binom{n}{2}} (-1)^n = q^{\binom{n}{2}} (-1)^n,$$

as required. Now that we completely characterized the Möbius function for all subspaces of $V_n(q)$, we are ready to prove the q-Möbius inversion formula.

Proposition 9.1. *The set of all subspaces of a vector space V forms a bounded lattice, where the partial ordering is defined as inclusion.*

Proof. The set of all subspaces of a vector space V has a unique minimum element $\emptyset$ and a unique maximum elements V. Thus it only remains to prove that the set of all spaces forms a lattice.

Let W_1 and W_2 be two subspaces of V. Then clearly, $W_1, W_2 \leq W_1 + W_2$, making it an upper bound of W_1 and W_2. Now suppose that W is another upper bound of W_1 and W_2. Suppose that $v \in W_1 + W_2$. Then there exist $v_1 \in W_1$ and $v_2 \in W_2$ such that $v = v_1 + v_2$. But since W is a supremum of W_1 and W_2, it follows that $v_1 \in W$ and $v_2 \in W$. Hence $v_1 + v_2 \in W$. Therefore, if W were another upper bound, then necessarily $W_1 + W_2 \subseteq W$. Hence $W_1 + W_2$ is the unique least upper bound of W_1 and W_2, making it the unique supremum of W_1 and W_2.

Now in a similar manner, we can prove that $W_1 \cap W_2$ is the unique infimum of W_1 and W_2. Clearly, since $W_1 \cap W_2 \subseteq W_1$ and W_2, it follows $W_1 \cap W_2$ is a lower bound of W_1 and W_2. Suppose that W' is another lower bound of W_1 and W_2. For any $w \in W$, we have $w \in W_1$ and $w \in W_2$, so $w \in W_1 \cap W_2$. This proves that $W \subseteq W_1 \cap W_2$, so $W_1 \cap W_2$ is the greatest lower bound of W_1 and W_2 as required. □

Theorem 9.2 (q-Möbius inversion formula)**.** *The following two are equivalent.*

(1) $g(n) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q f(k)$

(2) $f(n) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{k}{2}} (-1)^k g(n-k).$

Proof. Let $L_n(q)$ be the set of all subspaces of $V_n(q)$, which we know is a bounded lattice by Proposition 9.1. Let $N_{\leq}(W) : L_n(q) \to \mathbb{C}$ and $N_{=}(U) : L_n(q) \to \mathbb{C}$ be functions defined by

$$N_{\leq}(W) = \sum_{U \subseteq W} N_{=}(U).$$

Then by Theorem 8.6, we have

$$N_{=}(W) = \sum_{U \subseteq W} \mu(U,W) N_{\leq}(U).$$

Now letting $N_{\leq}(W) := g(\dim(W))$ and $N_{=}(W) := f(\dim(W))$ gives us

$$\begin{aligned} f(n) = N_{=}(V_n(q)) &= \sum_{U \subseteq V_n(q)} \mu(U, V_n(q)) N_{\leq}(U) = \sum_{k=0}^{n} \sum_{\substack{U_k \subseteq V_n(q) \\ \dim(U_k) = n-k}} \mu(U_k, V_n(q)) N_{\leq}(U_k) \\ &= \sum_{k=0}^{n} \sum_{\substack{U_k \subseteq V_n(q) \\ \dim(U_k) = n-k}} q^{\binom{k}{2}} (-1)^k g(n-k) = \sum_{k=0}^{n} \begin{bmatrix} n \\ n-k \end{bmatrix}_q q^{\binom{k}{2}} (-1)^k g(n-k) \\ &= \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{k}{2}} (-1)^k g(n-k), \end{aligned}$$

by Theorem 6.1 and the symmetric nature of q-binomial coefficients. □

9.3. Möbius function in number theory, revisited

For $\mathbb{N}$, it is straightforward to verify that the divisibility relation gives $\mathbb{N}$ a poset structure. On top of this, if we let $\wedge$ denote the gcd operation and $\vee$ the lcm operation, with the minimum element 1, we see that $(\mathbb{N}, \leq, \vee, \wedge, 0)$ confers a lattice structure on $\mathbb{N}$. This structure comes in handy, since the following theorem provides an easy way of computing the Möbius function for number theory from the poset counterpart. We will abuse the notation, and denote $\mu(n)$ the classical Möbius function, and $\mu(x, y)$ the poset Möbius function.

Theorem 9.3 (Weisner's theorem)**.** *Let μ be the Möbius function for a finite lattice $(L, \vee, \wedge, 0_L, 1_L)$, and let $a \in L$ such that $a > 0_L$. Then we have*

$$\sum_{x \vee a = 1_L} \mu(0_L, x) = 0.$$

Proof. Recall that

$$\sum_{c \leq z \leq d} \mu(c, z) = \sum_{c \leq z \leq d} \mu(z, d) = 0,$$

as long as $c \neq d$. Therefore, letting $c = x \vee a$ and $d = 1_L$ gives us

$$\begin{aligned} \sum_{x \vee a = 1_L} \mu(0_L, x) &= \sum_{x \in L} \mu(0_L, x) \left(\sum_{x \vee a \leq z \leq 1_L} \mu(z, 1_L) \right) = \sum_{x \in L} \sum_{a \leq z \leq 1_L} \zeta(x, z) \mu(0_L, x) \mu(z, 1_L) \\ &= \sum_{a \leq z \leq 1_L} \sum_{x \in L} \zeta(x, z) \mu(0_L, x) \mu(z, 1_L) = \sum_{a \leq z \leq 1_L} \mu(z, 1_L) \left(\sum_{x \in L} \zeta(x, z) \mu(0_L, x) \right) \\ &= \sum_{a \leq z \leq 1_L} \mu(z, 1_L) \underbrace{\sum_{0_L \leq x \leq z} \mu(0_L, x)}_{(*)}. \end{aligned}$$

Note that $(*)$ is 0 as long as $z \neq 0_L$. But since $0_L < a \leq z$, it follows that $(*)$ is indeed 0. The theorem follows. □

We will also introduce a notation used often in number theory that will come in handy.

Definition 9.2. We denote that $d \,\|\, n$ if d is a *unitary divisor* of n, i.e., $d \mid n$ and $\gcd(d, n/d) = 1$.

Theorem 9.4. *$\mu(a,b) = \mu(1, b/a)$ for all $a, b \in \mathbb{N}$, and $\mu(1,n) = n$. Therefore, $\mu(a,b) = \mu(b/a)$ for all $a, b \in \mathbb{N}$.*

Proof. For the first part, it suffices to show that $\mu(a, an) = \mu(1, n)$ for all $a, n \in \mathbb{N}$. If $n = 1$, then $\mu(a,a) = 1 = \mu(1,1)$, so the claim holds. Suppose that the claim holds for all $1 \leq d < n$. Then we see that

$$\mu(a, an) = -\sum_{\substack{a|x|an \\ x<an}} \mu(a,x) = -\sum_{\substack{ad|an \\ d<n}} \mu(a, ad),$$

but by the inductive hypothesis, we have $\mu(a, ad) = \mu(1, d)$. Therefore

$$\mu(a, an) = -\sum_{\substack{ad|an \\ d<n}} \mu(1,d) = -\sum_{\substack{d|n \\ d<n}} \mu(1,d) = \mu(1,n).$$

We will also prove that $\mu(1,n) = \mu(n)$ by induction. Clearly, if $n = 1$, then $\mu(1,1) = 1 = \mu(1)$. Let $b > 1$, and pick a prime p so that $p \,|\, b$. Then the divisors of b forms a finite lattice with respect to divisibility, so we can apply Theorem 9.3 here. It follows that

$$\sum_{\operatorname{lcm}(d,p)=b} \mu(1,d) = 0, \text{ so } \mu(1,b) = -\sum_{\substack{\operatorname{lcm}(d,p)=b \\ d\neq b}} \mu(1,d).$$

If $p^2 \mid b$, then there is no d such that $\operatorname{lcm}(d,p) = b$, so this produces the empty sum. If $p \,\|\, b$, then the only possible d is $d = b/p$. Therefore, by the inductive hypothesis, we have $\mu(1,b) = -\mu(1, b/p) = -\mu(b/p) = \mu(b)$ as required. □

9.4. Convolution in number theory: Dirichlet convolution[2]

In this section, we will discuss convolution under number-theoretic setting, and along the way, provide an alternative proof of the classical Möbius inversion formula using the Dirichlet series (even though it is an overkill). This involves using the incidence algebra structure of $\mathbb{N}$ coming from the divisibility partial order (more specifically, we are only interested in functions of the form $f(1,n)$ where $f \in \operatorname{ia}(\mathbb{N})$). The convolution defined in this context, called the *Dirichlet convolution*, enjoys special properties that may not hold in general posets (for instance, commutativity). First, we will define the Dirichet convolution, and then proceed to define the δ function and the ζ function under this setting.

Definition 9.3. Suppose f and g are arithmetical functions. Then the *Dirichlet convolution* of f and g is

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Observe that the Dirichlet convolution is a special case of the convolution for incidence algebras, but with the interval $[1, n]$. It is straightforward to verify that the δ function is

[2] I added in this section myself to tie the ideas from incidence algebras back to the more familiar number-theoretic settings, and to demonstrate how the theorem on the Dirichlet series for the convolution of two arithmetical functions was used to prove Theorem 8.3. If one is only interested in the contents formally covered in the summer school course, then one need not read this section.

precisely $\delta(n) = \delta_{n,1}$, since

$$(f * \delta)(n) = \sum_{d|n} f(d)\delta_{n/d,1} = f(n)\delta_{1,1} = f(n).$$

The ζ function (but we will use ζ' instead to avoid the confusion between the Riemann zeta function) must satisfy

$$(\mu * \zeta')(n) = \delta_{n,1}.$$

But recall that

$$\sum_{d|n} \mu(d) = \delta_{n,1} = \delta(n),$$

so $\zeta'(n) \equiv 1$ for all n. Therefore, we will from now on write $\mathbf{1}(n)$ instead to denote the function that is always 1.

Theorem 9.5. *Let M be the set of multiplicative arithmetical functions equipped with the convolution operation $*$. Then M forms an abelian group.*

Proof. Let $f, g \in M$. Associativity of convolutions is already proved. Note that $\mathbf{1}(n), \delta(n) \in M$, so M is non-empty. Thus it suffices to prove that there is $h \in M$ such that $f * h = \delta$, that $f * g \in M$, and that $f * g = g * f$. Let $\gcd(m, n) = 1$. Suppose that for $d \,|\, mn$, we write $s := \gcd(d, m)$ and $t := \gcd(d, n)$. Observe that $d = st$ since $\gcd(m, n) = 1$. On the other hand, if $s \,|\, m$ and $t \,|\, n$, then $d = st \,|\, mn$. So clearly $s = \gcd(d, m)$ and $t = \gcd(d, n)$. This implies that there is a one-to-one correspondence between the set of divisors of mn and the set of pairs (s, t) of divisors of m and n respectively. It follows that

$$\begin{aligned}(f * g)(mn) &= \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) = \sum_{s|m}\sum_{t|n} f(st) g\left(\frac{mn}{st}\right) \\ &= \sum_{s|m} f(s) g\left(\frac{m}{s}\right) \sum_{t|n} f(t) g\left(\frac{n}{t}\right) = [(f * g)(m)][(f * g)(n)].\end{aligned}$$

We may assume that $f(1) \neq 0$. Otherwise, we will have $f(n) = f(1)f(n) = 0$ for all n, which contradicts the fact that f cannot be identically zero. In fact, since $f(n) = f(n \cdot 1) = f(n)f(1)$, it follows that $f(1) = 1$ for all $f \in M$. Therefore by Proposition 8.1(3), there exists some arithmetical function f^{-*} such that $f * f^{-*} = f^{-*} * f = \delta$. Suppose that $h \in M$ such that $h = f^{-*}$ for all prime powers. Since h is multiplicative, h is completely determined by how h behaves across prime powers. But then $f * h$ is multiplicative, as we just showed, so

$$(f * h)(p^a) = (f * f^{-*})(p^a) = u(p^a),$$

since all the factors of p^a are prime powers anyway. This proves that $h \equiv f^{-*}$ everywhere, so h is indeed the inverse we are looking for. It is straightforward to verify commutativity: indeed,

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{ba=n} g(a)f(b) = (g * f)(n). \qquad \square$$

Corollary 9.1. *$\mu(n)$ is multiplicative.*

Proof. $\mu(n)$ is the convolution inverse of $\mathbf{1}(n)$. □

Theorem 9.6. *Let f and g be arithmetical functions, and that both $\sum f(n)n^{-s}$ and $\sum g(n)n^{-s}$ are absolutely convergent for $\operatorname{Re} s > \sigma$. Then the Dirichlet series for $f * g$ is*

$$\sum_{n=0}^{\infty} \frac{(f*g)(n)}{n^s} = \left(\sum_{m=0}^{\infty} \frac{f(m)}{m^s}\right)\left(\sum_{t=0}^{\infty} \frac{g(t)}{t^s}\right)$$

for all $\operatorname{Re} s > \sigma$. Thus the Dirichlet series for $f * g$ is absolutely convergent for all $\operatorname{Re} s > \sigma$ as well.

Proof. Note that we are free to rearrange the terms since both $f(m)m^{-s}$ and $g(t)t^{-s}$ are absolutely convergent.

$$\begin{aligned}\left(\sum_{m=1}^{\infty} f(m)m^{-s}\right)\left(\sum_{t=1}^{\infty} g(t)t^{-s}\right) &= \sum_{m=1}^{\infty}\sum_{k=1}^{\infty} f(m)g(t)(mt)^{-s} \\ &= \sum_{n=1}^{\infty}\left(\sum_{mt=n} f(m)g(t)\right)(mt)^{-s} = \sum_{n=1}^{\infty}(f*g)(n)n^{-s}.\end{aligned}$$

As for absolute convergence, note that

$$\begin{aligned}\sum_{n=1}^{\infty} |(f*g)(n)n^{-s}| &\le \sum_{n=1}^{\infty}\left(\sum_{mt=n} |f(m)|\cdot|g(t)|\right)|n|^{-s} \\ &\le \left(\sum_{m=1}^{\infty} |f(m)m^{-s}|\right)\left(\sum_{t=1}^{\infty} |g(t)t^{-s}|\right) < \infty\end{aligned}$$

since $\sum f(m)m^{-s}$ and $\sum g(t)t^{-s}$ are both absolutely convergent. □

Therefore, Theorem 9.6 provides one possible method to compute the Dirichlet series of an arithmetical function.

Corollary 9.2. $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}.$

Proof. Recall that $\mu * \mathbf{1} = \delta$, so we have

$$\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right)\left(\sum_{m=1}^{\infty} \frac{1}{m^s}\right) = \sum_{k=1}^{\infty} \frac{\delta(k)}{k^s} = 1.$$ □

We also need the following result regarding the Dirichlet series.

Theorem 9.7. *If both $\sum f(n)n^{-s}$ and $\sum g(n)n^{-s}$ are absolutely convergent for all s with sufficiently large real parts, and $\sum f(n)n^{-s} = \sum g(n)n^{-s}$, then we have $f(n) = g(n)$ for all $n \in \mathbb{N}$.*

Now we are ready to provide another proof of Möbius inversion formula.

Proof of Theorem 8.4. Note that

$$g(n) = \sum_{d|n} f(d)$$

is equivalent to saying that $g = f * \mathbf{1}$. Therefore it follows that, by Theorem 9.6,

$$\sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \left(\sum_{m=1}^{\infty} \frac{f(m)}{m^s} \right) \zeta(s).$$

Divide both sides by $\zeta(s)$ to get

$$\sum_{m=1}^{\infty} \frac{f(m)}{m^s} = \zeta(s)^{-1} \left(\sum_{n=1}^{\infty} \frac{g(n)}{n^s} \right) = \left(\sum_{t=1}^{\infty} \frac{\mu(t)}{t^s} \right) \left(\sum_{n=1}^{\infty} \frac{g(n)}{n^s} \right),$$

for all s whose real part is sufficiently large, so $f = \mu * g$ by Theorem 9.7. The reverse direction can be proved similarly, since we can just reverse our reasoning. □

We will finish the section with some classical results from elementary number theory involving convolution.

Theorem 9.8. *Let $\varphi(n) := |\{1 \le a \le n : \gcd(a, n) = 1\}|$, i.e., Euler's totient function, and $N(n) := n$. Then the following are true:*

(1) $\varphi * \mathbf{1} = N$;
(2) $\mu * N = \varphi$;
(3) $\frac{\mu}{N} * \mathbf{1} = \frac{\varphi}{N}$; and
(4) φ is multiplicative.

Proof. (1) We will group integers $1 \le m \le n$ based on $\gcd(m, n) = d$. The number of integers m between 1 and n such that $\gcd(m, n) = d$ is precisely equivalent to finding the number of $m' := m/d$ so that $\gcd(m', n/d) = 1$. There are precisely $\varphi(n/d)$ integers satisfying such condition. Since every integer must belong to one of the subdivided groups, it follows that

$$\sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d) = n,$$

as required. (2) follows upon applying Möbius inversion. (3) follows immediately by dividing both sides of (2) by n. (4) also is immediate since φ is the Dirichlet convolution of two multiplicative functions. □

Corollary 9.3. $\displaystyle\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$ *for all* $\operatorname{Re} s > 2$.

Theorem 9.9. *Let $\Lambda(n)$ be the von Mangoldt function, i.e.,*

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some } k \ge 1 \\ 0 & \text{otherwise.} \end{cases}$$

Then $\Lambda * \mathbf{1} = \log$. Since

$$\sum_{n=1}^{\infty} \frac{\log n}{n^s} = -\zeta'(s),$$

it follows that, for all $\operatorname{Re} s > 1$,

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}.$$

Proof. Let $n = p_1^{e_1} \cdots p_r^{e_r}$. Then

$$(\Lambda * \mathbf{1})(n) = \sum_{\substack{d \mid n \\ d \text{ prime power}}} \Lambda(d) = \sum_{j=1}^{r} e_j \log(p_j) = \sum_{j=1}^{r} \log(p_j^{e_j}) = \log\left(\prod_{j=1}^{r} p_j^{e_j}\right) = \log(n).$$

That the Dirichlet series for $\log n$ is $-\zeta'(s)$ follows from the term-by-term differentiation, which we can do since $\zeta(s)$ converges absolutely and uniformly for any s with $\operatorname{Re} s > 1$. Observe that the derivative of n^{-s} is $-n^{-s}\log(n)$, so we have

$$-\zeta'(s) = \sum_{n=1}^{\infty} \frac{\log n}{n^s}.$$

The last claim follows from Theorem 9.6. Indeed, observe that

$$\left(\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}\right)\zeta(s) = \left(\sum_{n=1}^{\infty} \frac{\log(n)}{n^s}\right) = -\zeta'(s),$$

so dividing both sides by $\zeta(s)$ gives the result. □

Proposition 9.2. *Let $\lambda(n)$ be the Liouville function, which counts the number of prime factors of n, counting multiplicity. Then*

(1) $\lambda * \mathbf{1}$ is the indicator function for squares, and
(2) $\mu^2 * \lambda = |\mu| * \lambda = \delta$.

Proof. Both λ and $\mathbf{1}$ are multiplicative, so $\lambda * \mathbf{1}$ is multiplicative as well. That said, it suffices to show it for prime powers. We divide into two cases: when $n = p^{2k}$ and when $n = p^{2k+1}$ ($k \in \mathbb{Z}_{\geq 0}$), where p is a prime. If $n = p^{2k}$, then we have

$$\begin{aligned}\sum_{i=0}^{2k} \lambda(p^i) &= (-1)^0 + (-1)^1 + (-1)^2 + \cdots + (-1)^{2k-1} + (-1)^{2k} \\ &= ((-1)^0 + (-1)^1) + \cdots + ((-1)^{2k-2} + (-1)^{2k-1}) + (-1)^{2k} \\ &= (1-1) + (1-1) + \cdots + (1-1) + 1 = 1.\end{aligned}$$

On the other hand, if $n = p^{2k+1}$, then we have

$$\begin{aligned}\sum_{i=0}^{2k+1} \lambda(p^i) &= (-1)^0 + (-1)^1 + (-1)^2 + \cdots + (-1)^{2k-1} + (-1)^{2k} + (-1)^{2k+1} \\ &= ((-1)^0 + (-1)^1 + \cdots + (-1)^{2k-1} + (-1)^{2k}) + (-1)^{2k+1} = 1 - 1 = 0.\end{aligned}$$

Therefore if n is not a square (i.e., the prime factorization of n contains an odd exponent), then $(\lambda * \mathbf{1})(n) = 0$; if every exponent in the prime factorization of n is even, then $(\lambda * \mathbf{1})(n) = 1$, as required.

For the second part, we first start by observing that μ^2 is multiplicative, and that $\mu^2 \equiv |\mu|$. For any $(m, n) = 1$, if at least one of m and n is not square-free then the claim is immediate, since $\mu^2(mn) = 0$, and at least one of $\mu^2(m)$ and $\mu^2(n)$ must be 0. For any square-free number k, the value of $\mu^2(k)$ is always 1; thus, for any co-prime square-free numbers, we have $\mu^2(mn) = 1 = \mu^2(m)\mu^2(n)$. Hence $\mu^2 * \lambda$ is multiplicative. So we only need to show that the claim holds for prime powers, and for 1. For $n := p^k$, we have

$$\begin{aligned}(\mu^2 * \lambda)(p^k) &= \sum_{i=0}^{k} \mu^2(p^i)\lambda(p^{k-i}) = \mu^2(1)\lambda(p^k) + \mu^2(p)\lambda(p^{k-1}) \\ &= (-1)^k + (-1)^{k-1} = 0.\end{aligned}$$

On the other hand, if $n = 1$, then $(\mu^2 * \lambda)(1) = \mu^2(1)\lambda(1) = 1 \cdot (-1)^0 = 1$. Thus, $(\mu^2 * \lambda)(n)$ is 1 for $n = 1$, and 0 for any other natural numbers, as required. □

Theorem 9.10. *We have*

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)} \text{ and } \sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} = \frac{\zeta(s)}{\zeta(2s)}$$

for all $\operatorname{Re} s > 1$.

Proof. Both are immediate from Proposition 9.2 and Theorem 9.6. Indeed, we have

$$\left(\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s}\right)\zeta(s) = \frac{1}{1^s} + \frac{1}{4^s} + \frac{1}{9^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^{2s}} = \zeta(2s),$$

so dividing both sides by $\zeta(s)$ gives the result. As for the second claim, note that, by the previous result,

$$\left(\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s}\right)\left(\sum_{t=1}^{\infty} \frac{\lambda(t)}{t^s}\right) = \left(\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s}\right)\frac{\zeta(2s)}{\zeta(s)} = 1,$$

so multiplying both sides by $\zeta(s)/\zeta(2s)$ gives us the desired result. □

References

[AAR99] G. E. Andrews, R. A. Askey, and R. Roy, *Special Functions*, Cambridge University Press, Cambridge, 1999.

[And71] G. E. Andrews, *Number Theory*, W. B. Saunders Company, Philadelphia, PA, USA, 1971.

[And98] ______, *The Theory of Partitions*, Cambridge University Press, Cambridge, 1998.

[BP06] C. Boulet and I. Pak, *A combinatorial proof of the Rogers–Ramanujan and Schur identities*, J. Combin. Theory Ser. A **113** (2006), no. 6, 1019–1030.

[GR04] G. Gaspar and M. Rahman, *Basic Hypergeometric Series*, 2nd ed., Cambridge University Press, Cambridge, 2004.

[Har40] G. H. Hardy, *Ramanujan. Twelve Lectures on Subjects Suggested by His Life and Work*, Cambridge University Press, Cambridge, UK, 1940.

[IS] M. E. H. Ismail and D. Stanton, *Introduction to Quantum Calculus.*

[ISV87] M. E. H. Ismail, D. Stanton, and G. Viennot, *The combinatorics of q-Hermite polynomials and the Askey–Wilson integral*, European J. Combin. **8** (1987), no. 4, 379–392.

Department of Mathematics and Statistics, Dalhousie University, 6316 Coburg Rd, Halifax, NS, Canada B3H 4R2

E-mail address: hsyang@dal.ca