Pentagonal Number Theorem

Jonathan Conrad Paula Muermann Maryna Viazovska

September 17, 2026

1 Partitions

Definition 1. A *partition* of a positive integer n, also called an integer partition, is a way of writing n as a sum of positive integers. Two sums that differ only in the order of their summands are considered the same partition.

The *partition function* $p(n)$ represents the number of possible partitions of a natural number n.

Example 2. $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$
$p(5) = 7$

Lemma 3. *The generating function for $p(n)$ is given by*

$$\sum_{n=0}^{\infty} p(n)\, x^n = \prod_{k=1}^{\infty}(1 + x^k + x^{2k} + ...) = \prod_{k=1}^{\infty}(1 - x^k)^{-1}.$$

Proof. We work in the ring of formal power series $\mathbb{Z}[[x]]$.

Step 1. For each fixed $k \geq 1$, the geometric series identity

$$1 + x^k + x^{2k} + \cdots = \sum_{j=0}^{\infty} x^{jk} = (1 - x^k)^{-1}$$

holds as formal power series. This gives the second equality.

Step 2. Expand the product $\prod_{k=1}^{\infty}(1+x^k+x^{2k}+\cdots)$. Each term in the expansion is obtained by selecting, for every $k \geq 1$, an exponent $j_k \in \mathbb{Z}_{\geq 0}$ (with $j_k = 0$ for all but finitely many k) and multiplying the chosen monomials. Such a selection contributes a single term

$$\prod_k x^{j_k \cdot k} = x^{\sum_k j_k \cdot k}.$$

Step 3. The coefficient of x^n is therefore the number of tuples $(j_1, j_2, ...)$ with $\sum_k k \cdot j_k = n$.

Step 4. Such a tuple corresponds bijectively to a partition of n: j_k is the multiplicity of the part k. Hence the coefficient of x^n equals $p(n)$, and the first equality follows. □

Definition 4 (Partitions of n into distinct parts)**.**

Let $n \in \mathbb{N}$. We define the following sets of partitions of n into distinct positive parts:

$$\mathcal{P}(n) = \left\{ S \subseteq \{1, \dots, n\} \;\middle|\; \sum_{s \in S} s = n \right\},$$
$$\mathcal{P}_{\text{even}}(n) = \{S \in \mathcal{P}(n) \mid |S| \equiv 0 \pmod 2\},$$
$$\mathcal{P}_{\text{odd}}(n) = \{S \in \mathcal{P}(n) \mid |S| \equiv 1 \pmod 2\}.$$

We further define the number of even and odd partitions of n as $p_e(n) = |\mathcal{P}_{\text{even}}(n)|$ and $p_o(n) = |\mathcal{P}_{\text{odd}}(n)|$.

Lemma 5. *We have*

$$\prod_{k=1}^{\infty}(1-x^k) \;=\; \sum_{s=0}^{\infty} \sum_{k_1<k_2<\cdots<k_s} (-1)^s\, x^{k_1+k_2+\cdots+k_s} \;=\; \sum_{n=0}^{\infty} c_n\, x^n$$

where $c_0 = 1$ *and* $c_n = p_e(n) - p_o(n)$ *for* $n \geq 1$.

Proof. We expand the infinite product as a formal power series.

Step 1: Expansion as a sum over finite subsets. For each $k \geq 1$, the factor $(1 - x^k)$ contributes either 1 or $-x^k$ when expanding the product. A choice across all factors corresponds to a finite subset

$$K = \{k_1 < k_2 < \cdots < k_s\} \subseteq \mathbb{Z}_{\geq 1}$$

(the indices for which $-x^k$ was selected). The contribution is

$$\prod_{k\in K}(-x^k) = (-1)^{|K|}\, x^{\sum_{k\in K} k} = (-1)^s\, x^{k_1+\cdots+k_s}.$$

Summing over all such K yields the first equality.

Step 2: Grouping by total exponent. A subset K of size s summing to n is exactly a partition $S \in \mathcal{P}(n)$ with $|S| = s$. Hence the coefficient of x^n equals

$$c_n = \sum_{S\in\mathcal{P}(n)} (-1)^{|S|}.$$

Step 3: $c_0 = 1$**.** Only $S = \emptyset$ partitions 0 into distinct positive parts, contributing $(-1)^0 = 1$.

Step 4: $c_n = p_e(n) - p_o(n)$ **for** $n \geq 1$**.** Splitting the sum by parity of $|S|$:

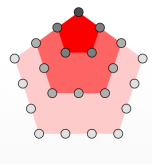
$$c_n = \sum_{\substack{S\in\mathcal{P}(n)\\ |S| \text{ even}}} 1 \;-\; \sum_{\substack{S\in\mathcal{P}(n)\\ |S| \text{ odd}}} 1 = |\mathcal{P}_{\text{even}}(n)| - |\mathcal{P}_{\text{odd}}(n)| = p_e(n) - p_o(n).$$

□

2 Pentagonal number theorem

Theorem 6 (Euler)**.**

$$\prod_{i=1}^{\infty}(1-x^i) \;=\; 1 + \sum_{k=1}^{\infty}(-1)^k\,(x^{(3k^2-k)/2} + x^{(3k^2+k)/2}) \;=\; \sum_{k\in\mathbb{Z}}(-1)^k\, x^{(3k^2-k)/2}.$$



k	-3	-2	-1	0	1	2	3
$\frac{3k^2-k}{2}$	15	7	2	0	1	5	12

The generalized pentagonal numbers $\frac{3k^2-k}{2}$, $k \in \mathbb{Z}$: $0, 1, 2, 5, 7, 12, 15, \ldots$; the nested pentagons depict the figurate pentagonal numbers $1, 5, 12, \ldots$ $(k \geq 1)$.

Proof. The proof combines the previous expansion lemma with the closed-form computation of $p_e(n) - p_o(n)$ via Franklin's involution.

Step 1: Coefficient identification. By Lemma 5,

$$\prod_{i=1}^{\infty}(1-x^i) = \sum_{n=0}^{\infty} c_n\, x^n,$$

where $c_0 = 1$ and $c_n = p_e(n) - p_o(n)$ for $n \geq 1$.

Step 2: Closed form for c_n. By Lemma 22 below,

$$p_e(n) - p_o(n) = \begin{cases} (-1)^k & \text{if } n = (3k^2-k)/2 \text{ for some } k \in \mathbb{Z}_{\geq 1}, \\ (-1)^k & \text{if } n = (3k^2+k)/2 \text{ for some } k \in \mathbb{Z}_{\geq 1}, \\ 0 & \text{otherwise.} \end{cases}$$

Step 3: Reassembling the sum. The values of n where $c_n \neq 0$ are exactly the (generalized) pentagonal numbers $n = (3k^2 \pm k)/2$ for $k \geq 1$, plus $n = 0$. Each contributes $(-1)^k$. Hence

$$\prod_{i=1}^{\infty}(1-x^i) = 1 + \sum_{k=1}^{\infty}(-1)^k \left(x^{(3k^2-k)/2} + x^{(3k^2+k)/2}\right).$$

Step 4: Bilateral sum reformulation. Reindex the second family by $k \mapsto -k$. For $k \in \mathbb{Z}_{\geq 1}$, set $k' = -k$, so $k' \in \mathbb{Z}_{\leq -1}$ and

$$\frac{3(k')^2 - k'}{2} = \frac{3k^2 + k}{2}, \qquad (-1)^k = (-1)^{|k'|} = (-1)^{k'}.$$

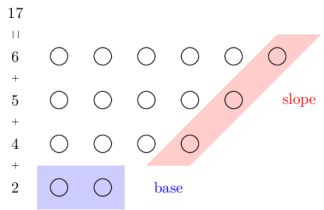
The $k = 0$ term gives $(-1)^0\, x^0 = 1$, matching the leading 1. Combining the three contributions:

$$\sum_{k \in \mathbb{Z}_{\geq 1}} (-1)^k x^{(3k^2-k)/2} \;+\; (-1)^0 x^0 \;+\; \sum_{k' \in \mathbb{Z}_{\leq -1}} (-1)^{k'} x^{(3(k')^2-k')/2} \;=\; \sum_{k \in \mathbb{Z}} (-1)^k x^{(3k^2-k)/2}.$$

□

2.1 Proof

Let n be a positive integer. Consider a diagram of a partition of n into different parts.



Definition 7 (Base and slope)**.** Consider a nonempty partition $S \subseteq \{1, \ldots, n\}$ of n into different parts. We define the *base* $b \in S$ as the smallest element of the partition, $b = \min(S)$. Let $\max(S)$ denote the largest element of S. We define the *slope* s as:

$$s = \max\{k \geq 1 : \max(S), \max(S) - 1, \max(S) - 2, \ldots, \max(S) - k + 1 \in S\}.$$

and the *slope set* D as $\{\max(S), \max(S) - 1, \ldots, \max(S) - s + 1\}$.

Definition 8. Let $n \in \mathbb{N}_{\geq 1}$ be a positive integer. Consider $S \in \mathcal{P}(n)$ nonempty with base b, slope s, and slope set D. We define the following sets of partitions of n into distinct positive parts:

$$\begin{aligned}
\mathcal{P}_{\alpha}(n) &= \left\{ S \in \mathcal{P}(n) \;\middle|\; S \neq \emptyset \text{ and } \left[(b \leq s \text{ and } b \notin D) \text{ or } b \leq s-1 \right] \right\}, \\
\mathcal{P}_{\beta}(n) &= \left\{ S \in \mathcal{P}(n) \;\middle|\; S \neq \emptyset \text{ and } \left[(b > s \text{ and } b \notin D) \text{ or } b \geq s+2 \right] \right\}, \\
\mathcal{P}_{\text{special}}(n) &= \left\{ S \in \mathcal{P}(n) \;\middle|\; S = \emptyset, \text{ or } \left[b \in D \text{ and } (b = s \text{ or } b = s+1) \right] \right\}.
\end{aligned}$$

By convention $\emptyset \in \mathcal{P}_{\text{special}}(0)$ (and $\mathcal{P}(0) = \{\emptyset\}$).

Lemma 9. *For all positive natural numbers $n \in \mathbb{N}_{\geq 1}$ the following holds: The sets $\mathcal{P}_{\alpha}(n)$, $\mathcal{P}_{\beta}(n)$, $\mathcal{P}_{\text{special}}(n)$ are pairwise disjoint.*

Proof. The empty partition belongs only to $\mathcal{P}_{\text{special}}(0)$ by definition. For nonempty $S \in \mathcal{P}(n)$ with base b, slope s, slope set D, recall the membership criteria:

- $S \in \mathcal{P}_{\alpha}$ iff $(b \leq s \text{ and } b \notin D)$ or $b \leq s-1$;
- $S \in \mathcal{P}_{\beta}$ iff $(b > s \text{ and } b \notin D)$ or $b \geq s+2$;
- $S \in \mathcal{P}_{\text{special}}$ iff $b \in D$ and $(b = s \text{ or } b = s+1)$.

Step 1: $\mathcal{P}_{\alpha} \cap \mathcal{P}_{\beta} = \emptyset$. Suppose $S \in \mathcal{P}_{\alpha} \cap \mathcal{P}_{\beta}$. Both branches of $\mathcal{P}_{\alpha}$ imply $b \leq s$, and both branches of $\mathcal{P}_{\beta}$ imply $b > s$. Contradiction.

Step 2: $\mathcal{P}_{\alpha} \cap \mathcal{P}_{\text{special}} = \emptyset$. Suppose $S \in \mathcal{P}_{\text{special}}$, so $b \in D$ and $b \in \{s, s+1\}$.

- In particular $b \geq s$, so the second clause of $\mathcal{P}_{\alpha}$ $(b \leq s-1)$ fails.
- The first clause requires $b \notin D$, but $b \in D$, so it also fails.

Hence $S \notin \mathcal{P}_{\alpha}$.

Step 3: $\mathcal{P}_{\beta} \cap \mathcal{P}_{\text{special}} = \emptyset$. Suppose $S \in \mathcal{P}_{\text{special}}$, so $b \in D$ and $b \leq s+1$.

- The second clause of $\mathcal{P}_{\beta}$ $(b \geq s+2)$ fails since $b \leq s+1$.
- The first clause requires $b \notin D$, contradicted by $b \in D$.

Hence $S \notin \mathcal{P}_{\beta}$. □

Lemma 10. *For all positive integer numbers n the following holds*

$$\mathcal{P}(n) = \mathcal{P}_{\alpha}(n) \sqcup \mathcal{P}_{\beta}(n) \sqcup \mathcal{P}_{\text{special}}(n).$$

Proof. By Lemma 9 the three sets are pairwise disjoint, so it suffices to show that every $S \in \mathcal{P}(n)$ belongs to at least one of them.

Step 1: Edge case $S = \emptyset$. This occurs only when $n = 0$. By Definition 8, $\emptyset \in \mathcal{P}_{\text{special}}(0)$.

Step 2: Main case ($S \neq \emptyset$). Let $b = \min(S)$, s the slope, D the slope set. We consider four cases on b vs s:

Case 1: $b \leq s-1$. The second clause of $\mathcal{P}_{\alpha}$ holds, so $S \in \mathcal{P}_{\alpha}$.

Case 2: $b = s$.

- If $b \notin D$: the first clause of $\mathcal{P}_{\alpha}$ $(b \leq s \text{ and } b \notin D)$ holds, so $S \in \mathcal{P}_{\alpha}$.
- If $b \in D$: then $b = s$ and $b \in D$, so $S \in \mathcal{P}_{\text{special}}$.

Case 3: $b = s + 1$**.**

- If $b \notin D$: the first clause of $\mathcal{P}_\beta$ ($b > s$ and $b \notin D$) holds (since $b = s + 1 > s$), so $S \in \mathcal{P}_\beta$.
- If $b \in D$: then $b = s + 1$ and $b \in D$, so $S \in \mathcal{P}_{\text{special}}$.

Case 4: $b \geq s + 2$**.** The second clause of $\mathcal{P}_\beta$ holds, so $S \in \mathcal{P}_\beta$.
These four cases cover all possibilities. □

Definition 11. For $k \in \mathbb{N}_{\geq 1}$ define $S_{-k} = \{k, k+1, \ldots, 2k-1\}$ (a set of k elements summing to $(3k^2 - k)/2$).
For $k \in \mathbb{N}_{\geq 1}$ define $S_k = \{k+1, k+2, \ldots, 2k\}$ (a set of k elements summing to $(3k^2 + k)/2$).

Lemma 12. *For $n \in \mathbb{N}_{\geq 1}$:*

- *If n is not a pentagonal number, then $\mathcal{P}_{\text{special}}(n) = \emptyset$.*
- *If $n = \frac{3k^2-k}{2}$ for some $k \in \mathbb{Z}_{\geq 1}$, then $\mathcal{P}_{\text{special}}(n) = \{S_{-k}\}$.*
- *If $n = \frac{3k^2+k}{2}$ for some $k \in \mathbb{Z}_{\geq 1}$, then $\mathcal{P}_{\text{special}}(n) = \{S_k\}$.*

For $n = 0$, $\mathcal{P}_{\text{special}}(0) = \{\emptyset\}$ by convention.

Proof. The case $n = 0$ holds by Definition 8. Assume $n \geq 1$, so any $S \in \mathcal{P}_{\text{special}}(n)$ is nonempty.

Step 1: Structure of a special partition. Let $S \in \mathcal{P}_{\text{special}}(n)$ with base b, slope s, slope set D. By definition, $b \in D$ and either $b = s$ or $b = s + 1$.

Sub-step 1a: $S = D$**.** The slope set is the maximal top-consecutive run: $D = \{\max(S) - s + 1, \ldots, \max(S)\}$. Since $b \in D$, we have $b \geq \max(S) - s + 1$, so $\{b, b+1, \ldots, \max(S)\} \subseteq D \subseteq S$. Combined with $b = \min(S)$, this forces

$$S = \{b, b+1, \ldots, \max(S)\} = D.$$

In particular $|S| = \max(S) - b + 1 = s$, so $\max(S) = b + s - 1$.

Step 2: Case A ($b = s$)**.** Then $|S| = s = b$ and $\max(S) = 2b - 1$, so

$$S = \{b, b+1, \ldots, 2b-1\}.$$

The sum is

$$\sum_{i=b}^{2b-1} i = b \cdot b + (0 + 1 + \cdots + (b-1)) = b^2 + \frac{b(b-1)}{2} = \frac{3b^2 - b}{2}.$$

Setting $k = b \in \mathbb{Z}_{\geq 1}$, we have $n = (3k^2 - k)/2$ and $S = S_{-k} = \{k, k+1, \ldots, 2k-1\}$.

Step 3: Case B ($b = s + 1$)**.** Then $|S| = s = b - 1$ and $\max(S) = b + s - 1 = 2b - 2$, so

$$S = \{b, b+1, \ldots, 2b-2\}.$$

The sum is

$$\sum_{i=b}^{2b-2} i = (b-1) \cdot b + (0 + 1 + \cdots + (b-2)) = b(b-1) + \frac{(b-1)(b-2)}{2} = \frac{(b-1)(3b-2)}{2}.$$

Setting $k = b - 1 \in \mathbb{Z}_{\geq 1}$ (note $b \geq 2$ since $s \geq 1$), we get

$$n = \frac{k(3(k+1) - 2)}{2} = \frac{k(3k+1)}{2} = \frac{3k^2 + k}{2}, \qquad S = \{k+1, k+2, \ldots, 2k\} = S_k.$$

Step 4: Forward direction (existence). Conversely, given $n = (3k^2 - k)/2$ with $k \geq 1$, the set $S_{-k} = \{k, k+1, \ldots, 2k-1\}$ has base k, slope k (the entire set is a top-consecutive run of length k), slope set $D = S_{-k}$, and $b = k \in D$ with $b = s$, hence $S_{-k} \in \mathcal{P}_{\text{special}}$. Similarly, $S_k = \{k+1, \ldots, 2k\}$ has base $k+1$, slope k, slope set $D = S_k$, and $b = k+1 = s+1 \in D$, hence $S_k \in \mathcal{P}_{\text{special}}$.

Step 5: Uniqueness. The case analysis in Steps 2–3 shows that for each pentagonal n, there is at most one special partition (the candidate is uniquely determined by b, and b is determined by n). Combined with Step 4, this gives exactly one.

Step 6: Non-pentagonal n. If n is not pentagonal of either form, then by Steps 2–3 no $b \geq 1$ produces a special partition with the sum equal to n, so $\mathcal{P}_{\text{special}}(n) = \emptyset$. □

Definition 13 (Operations α and β)**.** Let $S \subseteq \{1, \ldots, n\}$ be a nonempty partition of n into different parts with base b, slope s, max $m = \max(S)$, and slope set D. We define:

α: For $S \in \mathcal{P}_\alpha(n)$ (equivalently, $b \leq s$ and $b \notin D$, or $b \leq s-1$):

$$\alpha(S) = (S \setminus \{b,\, m-b+1\}) \cup \{m+1\}.$$

β: For $S \in \mathcal{P}_\beta(n)$ (equivalently, $b > s$ and $b \notin D$, or $b \geq s+2$):

$$\beta(S) = (S \cup \{s,\, m-s\}) \setminus \{m\}.$$

α

β

Lemma 14. *If $S \in \mathcal{P}_\alpha(n)$ then $\alpha(S) \in \mathcal{P}_\beta(n)$.*

Proof. Let $S \in \mathcal{P}_\alpha(n)$ with base b, slope s, max $m = \max(S)$, slope set $D = \{m-s+1, \ldots, m\}$. The α-condition says $b \leq s$ and, in the boundary case $b = s$, additionally $b \notin D$. Recall

$$\alpha(S) = (S \setminus \{b, m-b+1\}) \cup \{m+1\}.$$

Step 0: Key inequality $m \geq 2b$. We claim $m \geq 2b$ in both clauses of $\mathcal{P}_\alpha$. The top-b slope elements $\{m-b+1, \ldots, m\}$ lie in D (since $b \leq s$), so all are in S and all are $\geq m-b+1$.

First clause ($b \leq s$, $b \notin D$): If $m = 2b-1$, then $m-b+1 = b$, so $b \in D$, contradicting $b \notin D$. Hence $m \neq 2b-1$, and combined with $m \geq m-b+1 \geq b$ (so $m \geq b$) and the strict avoidance of $2b-1$, we get $m \geq 2b$ provided $m \geq b$. Actually we need $m \geq 2b-1$ first: since $\{m-b+1, \ldots, m\}$ has b distinct positive elements, $m-b+1 \geq 1$ gives $m \geq b$; combined with the existence of $b \in S$ and $b \notin D$, we have $b \leq m-b$ (since $b < m-b+1 = \min(D)$), giving $m \geq 2b$.

Second clause ($b \leq s-1$): Since $D \subseteq S$ and $b = \min(S)$, we have $b \leq \min(D) = m-s+1$. Therefore, $m \geq b+s-1$. Since $s \geq b+1$, it follows that $m \geq b+s-1 \geq b+(b+1)-1 = 2b$.

Step 1: $\alpha(S)$ is a partition of n. The sum change is $-b-(m-b+1)+(m+1) = 0$, so the sum is preserved. We must verify that $\alpha(S)$ has distinct positive elements.

- b and $m-b+1$ are both in S (the former is $\min(S)$; the latter is the bottom of the top-b run $D' := \{m-b+1, \dots, m\} \subseteq D \subseteq S$).
- $b \neq m-b+1$: by Step 0, $m \geq 2b$, so $m-b+1 \geq b+1 > b$.
- $m+1 \notin S$ since $m = \max(S)$, hence $m+1 \notin S \setminus \{b, m-b+1\}$.
- All elements are positive: $m+1 \geq 2$ and retained elements are ≥ 1.

Step 2: New extremes.

- New maximum: $m' := \max(\alpha(S)) = m+1$ (since $m+1$ exceeds every element of S).
- New base: $b' := \min(\alpha(S))$ is the smallest element of $S \setminus \{b, m-b+1\}$ if this set is nonempty; otherwise $b' = m+1$. Since all distinct elements of S are $\geq b$ and $\neq b$, we have $b' \geq b+1$.

Step 3: New slope s' and slope set D'. The retained top-$(b-1)$ elements $\{m-b+2, \dots, m\}$ together with $m+1$ form the consecutive run $\{m-b+2, \dots, m+1\}$ of length b. We claim this is the entire new slope, i.e., $s' = b$ and $D' = \{m-b+2, \dots, m+1\}$.

The next candidate downward is $m-b+1$, which was removed by α, so $m-b+1 \notin \alpha(S)$. Hence the top run terminates and $s' = b$, $D' = \{m-b+2, \dots, m+1\}$.

Step 4: Verify $\alpha(S) \in \mathcal{P}_\beta(n)$. We must show $b' > s' = b$ (with $b' \notin D'$ in the boundary case $b' = b+1$), or $b' \geq s'+2 = b+2$.

From Step 2, $b' \geq b+1$.

Subcase (i): $b' \geq b+2$. Then $b' \geq s'+2$, second clause of $\mathcal{P}_\beta$ holds.

Subcase (ii): $b' = b+1$. We need $b' \notin D'$. We have $D' = \{m-b+2, \dots, m+1\}$. By Step 0, $m \geq 2b$, so $m-b+2 \geq b+2 > b+1 = b'$. Hence $b' < \min(D')$, so $b' \notin D'$, first clause of $\mathcal{P}_\beta$ holds.

In both subcases, $\alpha(S) \in \mathcal{P}_\beta(n)$.

□

Lemma 15. *If $S \in \mathcal{P}_\beta(n)$ then $\beta(S) \in \mathcal{P}_\alpha(n)$.*

Proof. Let $S \in \mathcal{P}_\beta(n)$ with base b, slope s, max m, slope set $D = \{m-s+1, \dots, m\}$. Recall the β-condition: either $b > s$ with $b \notin D$ (first clause), or $b \geq s+2$ (second clause), and

$$\beta(S) = (S \cup \{s, m-s\}) \setminus \{m\}.$$

Step 0: Key inequality $m \geq 2s+1$. Since $D \subseteq S$ and $b = \min(S)$, we have $b \leq \min(D) = m-s+1$.

- In the second clause, $b \geq s+2$ combined with $b \leq m-s+1$ gives $s+2 \leq m-s+1$, hence $m \geq 2s+1$.
- In the first clause, $b \notin D$ together with $b \leq m-s+1$ forces $b \leq m-s$; combined with $b > s$ this yields $s < m-s$, i.e. $m \geq 2s+1$.

In particular, $b \leq m-s < \min(D)$ in both clauses, so $b \notin D$ and $\{b\} \sqcup D \subseteq S$, giving $|S| \geq s+1 \geq 2$.

Step 1: $\beta(S)$ is a partition of n. The sum change is $-m+s+(m-s) = 0$. For distinctness of the resulting set:

- $s \notin S \setminus \{m\}$: since $b > s$ and $b = \min(S)$, no element of S equals s.

- $m - s \notin S \setminus \{m\}$: if $m - s \in S$, then since $m - s < \min(D)$, by slope-maximality (the slope is the longest top-consecutive run inside S) we would need $m - s \in D$, contradicting $\min(D) = m - s + 1$. Also $m - s \neq m$ since $s \geq 1$.
- $s \neq m - s$: by Step 0, $m \geq 2s + 1 > 2s$.
- Positivity: $s \geq 1$, and $m - s \geq s + 1 \geq 2$.

Step 2: New extremes. The new base is

$$b' := \min(\beta(S)) = \min(b, s) = s,$$

since $b > s$. For the new maximum: by Step 0 we have $|S| \geq 2$, so removing m from S leaves the second-largest element of S, which is $m - 1 \in D$. The newly added elements s and $m - s$ are both at most $m - 1$ (using $m \geq 2s + 1$), so

$$m' := \max(\beta(S)) = m - 1.$$

Step 3: New slope and slope set. The shifted top run $\{m - s, m - s + 1, \dots, m - 1\}$ has length s and lies in $\beta(S)$. We split on the value of $m - 2s$.

Case (a): $m \geq 2s+2$. Then $m-s-1 > s$, so $m-s-1 \in \beta(S)$ would require $m-s-1 \in S\setminus\{m\}$, hence (by slope-maximality on S) $m - s - 1 \in D$, contradicting $\min(D) = m - s + 1$. The top run therefore terminates at $m - s$, giving

$$s' = s, \qquad D' = \{m - s, \dots, m - 1\}.$$

Case (b): $m = 2s + 1$. Then $m - s - 1 = s$, which is precisely the new bottom element added by β. The top run extends by one to include it:

$$s' = s + 1, \qquad D' = \{s, s + 1, \dots, 2s\}.$$

Step 4: Verify $\beta(S) \in \mathcal{P}_\alpha(n)$.

Case (a): $m \geq 2s + 2$. Here $b' = s$ and $s' = s$, so $b' = s'$ and the second clause $b' \leq s' - 1$ fails. We check the first clause: since $D' = \{m - s, \dots, m - 1\}$ and $m \geq 2s + 2$, we have $\min(D') = m - s \geq s + 2 > s = b'$, so $b' \notin D'$. Hence $\beta(S) \in \mathcal{P}_\alpha(n)$ via the first clause.

Case (b): $m = 2s + 1$. Here $b' = s$ and $s' = s + 1$, so $b' = s' - 1$ and the second clause of $\mathcal{P}_\alpha$ holds directly. Hence $\beta(S) \in \mathcal{P}_\alpha(n)$.

In both cases, $\beta(S) \in \mathcal{P}_\alpha(n)$. □

Lemma 16. *The composition of maps $\beta \circ \alpha$ is equal to the identity map on $\mathcal{P}_\alpha(n)$. Equivalently, if $S \in \mathcal{P}_\alpha(n)$ then $\beta(\alpha(S)) = S$.*

Proof. Let $S \in \mathcal{P}_\alpha(n)$ with base b, slope s, max m, slope set D.

Step 1: Compute $\alpha(S)$. By definition,

$$\alpha(S) = (S \setminus \{b, m - b + 1\}) \cup \{m + 1\}.$$

By Lemma 14, $\alpha(S) \in \mathcal{P}_\beta(n)$. From the proof of that lemma, the data of $\alpha(S)$ is:

- new max $m^\alpha = m + 1$,
- new slope $s^\alpha = b$ (the run $\{m - b + 2, \dots, m + 1\}$),
- new slope set $D^\alpha = \{m - b + 2, \dots, m + 1\}$.

Step 2: Apply β to $\alpha(S)$. By definition,

$$\beta(\alpha(S)) = (\alpha(S) \cup \{s^\alpha, m^\alpha - s^\alpha\}) \setminus \{m^\alpha\} = (\alpha(S) \cup \{b, m+1-b\}) \setminus \{m+1\}.$$

Step 3: Simplify. Substituting $\alpha(S) = (S \setminus \{b, m-b+1\}) \cup \{m+1\}$:

$$\begin{aligned}\beta(\alpha(S)) &= [((S \setminus \{b, m-b+1\}) \cup \{m+1\}) \cup \{b, m-b+1\}] \setminus \{m+1\} \\ &= [(S \setminus \{b, m-b+1\}) \cup \{b, m-b+1, m+1\}] \setminus \{m+1\} \\ &= (S \setminus \{b, m-b+1\}) \cup \{b, m-b+1\} \\ &= S,\end{aligned}$$

where we used that b and $m-b+1$ are in S (so re-adding them after removal recovers S), and that $m+1 \notin S \setminus \{b, m-b+1\}$ (since $m+1 > m \geq$ every element of S). □

Lemma 17. *The composition of maps $\alpha \circ \beta$ is equal to the identity map on $\mathcal{P}_\beta(n)$. Equivalently, if $S \in \mathcal{P}_\beta(n)$ then $\alpha(\beta(S)) = S$.*

Proof. Let $S \in \mathcal{P}_\beta(n)$ with base b, slope s, max m, slope set D.

Step 1: Compute $\beta(S)$.

$$\beta(S) = (S \cup \{s, m-s\}) \setminus \{m\}.$$

By Lemma 15, $\beta(S) \in \mathcal{P}_\alpha(n)$. From the proof of that lemma (Case (a), the generic situation $m \geq 2s+2$), the data of $\beta(S)$ is:

- new max $m^\beta = m-1$,
- new base $b^\beta = s$,
- new slope $s^\beta = s$ (the run $\{m-s, \dots, m-1\}$),
- new slope set $D^\beta = \{m-s, \dots, m-1\}$.

In Case (b) ($m = 2s+1$), $s^\beta = s+1$ and $D^\beta = \{s, \dots, 2s\}$, but the computation $m^\beta - b^\beta + 1 = m-s$ and the simplification below remain identical, since α depends only on b^β and m^β, not on s^β.

Step 2: Apply α to $\beta(S)$.

$$\alpha(\beta(S)) = (\beta(S) \setminus \{b^\beta, m^\beta - b^\beta + 1\}) \cup \{m^\beta + 1\} = (\beta(S) \setminus \{s, m-s\}) \cup \{m\}.$$

(Using $b^\beta = s$, $m^\beta = m-1$, so $m^\beta - b^\beta + 1 = m - 1 - s + 1 = m - s$.)

Step 3: Simplify. Substituting $\beta(S) = (S \cup \{s, m-s\}) \setminus \{m\}$:

$$\begin{aligned}\alpha(\beta(S)) &= [((S \cup \{s, m-s\}) \setminus \{m\}) \setminus \{s, m-s\}] \cup \{m\} \\ &= [(S \setminus \{m\}) \setminus \{s, m-s\}] \cup \{m\}.\end{aligned}$$

Since $s \notin S$ and $m - s \notin S$ (verified in the proof of Lemma 15), removing them from $S \setminus \{m\}$ has no effect:

$$\alpha(\beta(S)) = (S \setminus \{m\}) \cup \{m\} = S,$$

since $m \in S$. □

Lemma 18. *The map $\alpha : \mathcal{P}_\alpha(n) \to \mathcal{P}_\beta(n)$ is a bijection.*
The map $\beta : \mathcal{P}_\beta(n) \to \mathcal{P}_\alpha(n)$ is a bijection.

Proof. Lemma 14 shows α is well-defined as a map $\mathcal{P}_\alpha(n) \to \mathcal{P}_\beta(n)$, and Lemma 15 shows β is well-defined as a map $\mathcal{P}_\beta(n) \to \mathcal{P}_\alpha(n)$.

Lemma 16 gives $\beta \circ \alpha = \mathrm{id}_{\mathcal{P}_\alpha(n)}$, and Lemma 17 gives $\alpha \circ \beta = \mathrm{id}_{\mathcal{P}_\beta(n)}$.

Hence α and β are mutually inverse bijections. □

Lemma 19.

$$|\mathcal{P}_\alpha(n)| = \left|\mathcal{P}_\beta(n)\right|.$$

Proof. A bijection between finite sets implies equal cardinality. Apply this to the bijection $\alpha : \mathcal{P}_\alpha(n) \to \mathcal{P}_\beta(n)$ from Lemma 18. □

Lemma 20. *The operations α and β change the parity of the number of parts of a partition. More precisely,*

- *If $S \in \mathcal{P}_\alpha(n) \cap \mathcal{P}_{\mathrm{odd}}(n)$ then $\alpha(S) \in \mathcal{P}_\beta(n) \cap \mathcal{P}_{\mathrm{even}}(n)$;*
- *If $S \in \mathcal{P}_\alpha(n) \cap \mathcal{P}_{\mathrm{even}}(n)$ then $\alpha(S) \in \mathcal{P}_\beta(n) \cap \mathcal{P}_{\mathrm{odd}}(n)$;*
- *If $S \in \mathcal{P}_\beta(n) \cap \mathcal{P}_{\mathrm{odd}}(n)$ then $\beta(S) \in \mathcal{P}_\alpha(n) \cap \mathcal{P}_{\mathrm{even}}(n)$;*
- *If $S \in \mathcal{P}_\beta(n) \cap \mathcal{P}_{\mathrm{even}}(n)$ then $\beta(S) \in \mathcal{P}_\alpha(n) \cap \mathcal{P}_{\mathrm{odd}}(n)$.*

Proof. Membership in $\mathcal{P}_\beta$ for $\alpha(S)$ (and in $\mathcal{P}_\alpha$ for $\beta(S)$) is supplied by Lemmas 14 and 15. It remains to show that the parity of the number of parts is flipped.

Step 1: $|\alpha(S)| = |S| - 1$**.** By the definition $\alpha(S) = (S \setminus \{b, m-b+1\}) \cup \{m+1\}$:

- we remove two distinct elements (b and $m-b+1$, distinct as shown in the proof of Lemma 14), reducing the size by 2;
- we add one element ($m+1$), which is not in $S \setminus \{b, m-b+1\}$ since $m+1 > \max(S)$.

Net change: $-2+1 = -1$. So $|\alpha(S)| = |S| - 1$, flipping parity.

Step 2: $|\beta(S)| = |S| + 1$**.** By the definition $\beta(S) = (S \cup \{s, m-s\}) \setminus \{m\}$:

- we add two distinct new elements s and $m-s$ (distinct, and not in S, as verified in the proof of Lemma 15), increasing the size by 2;
- we remove one element ($m \in S$), reducing by 1.

Net change: $+2-1 = +1$. So $|\beta(S)| = |S| + 1$, flipping parity.

Step 3: Conclusion.

- $S \in \mathcal{P}_{\mathrm{odd}}$ means $|S|$ is odd; then $|\alpha(S)| = |S| - 1$ is even, so $\alpha(S) \in \mathcal{P}_{\mathrm{even}}$.
- $S \in \mathcal{P}_{\mathrm{even}}$ means $|S|$ is even; then $|\alpha(S)| = |S| - 1$ is odd, so $\alpha(S) \in \mathcal{P}_{\mathrm{odd}}$.
- Symmetrically for β with $|\beta(S)| = |S| + 1$.

□

Lemma 21.

$$|\mathcal{P}_\alpha(n) \cap \mathcal{P}_{\mathrm{odd}}(n)| = \left|\mathcal{P}_\beta(n) \cap \mathcal{P}_{\mathrm{even}}(n)\right|,$$
$$|\mathcal{P}_\alpha(n) \cap \mathcal{P}_{\mathrm{even}}(n)| = \left|\mathcal{P}_\beta(n) \cap \mathcal{P}_{\mathrm{odd}}(n)\right|.$$

Proof. Lemma 20 shows that α restricts to bijections $\mathcal{P}_\alpha(n) \cap \mathcal{P}_{\text{odd}}(n) \to \mathcal{P}_\beta(n) \cap \mathcal{P}_{\text{even}}(n)$ and $\mathcal{P}_\alpha(n) \cap \mathcal{P}_{\text{even}}(n) \to \mathcal{P}_\beta(n) \cap \mathcal{P}_{\text{odd}}(n)$ (with inverse β, by Lemma 18). Equal cardinalities follow. □

Lemma 22.

$$p_e(n) - p_o(n) = \begin{cases} (-1)^k, & \text{if } n = \frac{3k^2 \pm k}{2} \text{ for some } k \in \mathbb{Z}_{\geq 1}, \\ 1, & \text{if } n = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. **Step 0:** $n = 0$**.** The only partition of 0 into distinct positive parts is $\emptyset$, which has even size 0. So $p_e(0) = 1$, $p_o(0) = 0$, and $p_e(0) - p_o(0) = 1 = (-1)^0$.

Step 1: Reduction to special partitions. For $n \geq 1$,

$$p_e(n) - p_o(n) = |\mathcal{P}_{\text{even}}(n)| - |\mathcal{P}_{\text{odd}}(n)|\,. \tag{1}$$

By Lemma 10 we have

$$|\mathcal{P}_{\text{even}}(n)| = |\mathcal{P}_{\text{even}}(n) \cap \mathcal{P}_\alpha(n)| + \left|\mathcal{P}_{\text{even}}(n) \cap \mathcal{P}_\beta(n)\right| + \left|\mathcal{P}_{\text{even}}(n) \cap \mathcal{P}_{\text{special}}(n)\right|$$

and

$$|\mathcal{P}_{\text{odd}}(n)| = |\mathcal{P}_{\text{odd}}(n) \cap \mathcal{P}_\alpha(n)| + \left|\mathcal{P}_{\text{odd}}(n) \cap \mathcal{P}_\beta(n)\right| + \left|\mathcal{P}_{\text{odd}}(n) \cap \mathcal{P}_{\text{special}}(n)\right|.$$

By Lemma 21, $|\mathcal{P}_{\text{even}} \cap \mathcal{P}_\alpha| = |\mathcal{P}_{\text{odd}} \cap \mathcal{P}_\beta|$ and $|\mathcal{P}_{\text{odd}} \cap \mathcal{P}_\alpha| = |\mathcal{P}_{\text{even}} \cap \mathcal{P}_\beta|$. Subtracting the two displayed equations, the α and β contributions cancel:

$$|\mathcal{P}_{\text{even}}(n)| - |\mathcal{P}_{\text{odd}}(n)| = \left|\mathcal{P}_{\text{even}}(n) \cap \mathcal{P}_{\text{special}}(n)\right| - \left|\mathcal{P}_{\text{odd}}(n) \cap \mathcal{P}_{\text{special}}(n)\right|. \tag{2}$$

Step 2: Compute the special contribution. By Lemma 12, for $n \geq 1$:

- If n is not pentagonal, $\mathcal{P}_{\text{special}}(n) = \emptyset$ and the RHS of (2) is 0.
- If $n = (3k^2 - k)/2$ with $k \geq 1$, then $\mathcal{P}_{\text{special}}(n) = \{S_{-k}\}$ with $|S_{-k}| = k$. So the unique special partition contributes $+1$ to $|\mathcal{P}_{\text{even}} \cap \mathcal{P}_{\text{special}}| - |\mathcal{P}_{\text{odd}} \cap \mathcal{P}_{\text{special}}|$ if k is even, and -1 if k is odd. Hence the RHS of (2) equals $(-1)^k$.
- If $n = (3k^2 + k)/2$ with $k \geq 1$, then $\mathcal{P}_{\text{special}}(n) = \{S_k\}$ with $|S_k| = k$. Same computation: RHS equals $(-1)^k$.

Combining with (1), the lemma follows. □

3 The q-binomial theorem: statement and proof

3.1 Statement

Define the *finite* q-Pochhammer symbol

$$(a;q)_n = \prod_{k=0}^{n-1}(1 - aq^k), \qquad (a;q)_0 = 1,$$

the *q-factorial* $[n]_q! = (q;q)_n/(1-q)^n$, and the *Gaussian binomial coefficient*

$$\binom{n}{k}_q = \frac{(q;q)_n}{(q;q)_k\,(q;q)_{n-k}} \qquad (0 \leq k \leq n).$$

By convention $\binom{n}{k}_q = 0$ for $k < 0$ or $k > n$. These are polynomials in q with integer coefficients (this is part of what needs to be proved).

Theorem 23 (Finite q-binomial theorem)**.** *In $\mathbb{Z}[q, z]$, for every $n \geq 0$,*

$$\prod_{k=0}^{n-1}(1 + zq^k) = \sum_{k=0}^{n} q^{\binom{k}{2}} \binom{n}{k}_q z^k.$$

Theorem 24 (Infinite q-binomial / Cauchy identity)**.** *For $|q| < 1$ and any $a, z \in \mathbb{C}$ with $|z| < 1$,*

$$\sum_{n=0}^{\infty} \frac{(a;q)_n}{(q;q)_n} z^n = \frac{(az;q)_\infty}{(z;q)_\infty}.$$

The two Euler identities follow from Theorem 24 by specializing $a = 0$ (gives $1/(z;q)_\infty = \sum z^n/(q;q)_n$) and by sending $a \to \infty$ along $a = -y/q^N$ with $N \to \infty$, then renaming (gives $(-z;q)_\infty = \sum q^{\binom{n}{2}} z^n/(q;q)_n$).

3.2 Proof of the finite q-binomial theorem

This proof is purely algebraic (no analysis) and is the version best suited for Lean. It uses only induction on n and the q-Pascal identity.

Lemma 25 (q-Pascal)**.** *For all $n, k \in \mathbb{N}$,*

$$\binom{n+1}{k+1}_q = \binom{n}{k+1}_q + q^{n-k}\binom{n}{k}_q.$$

(Equivalently, with $k \geq 1$: $\binom{n+1}{k}_q = \binom{n}{k}_q + q^{n-k+1}\binom{n}{k-1}_q$. A symmetric form $\binom{n+1}{k+1}_q = q^{k+1}\binom{n}{k+1}_q + \binom{n}{k}_q$ also holds; we use the first.)

Proof. This is the recursive defining equation of $\binom{n}{k}_q$ in Definition 29, hence `rfl` in Lean. Equivalently, by direct computation from the quotient form $\binom{n}{k}_q = (q;q)_n/((q;q)_k(q;q)_{n-k})$ (valid when $k \leq n$ and the denominators are nonzero): $\binom{n}{k}_q + q^{n-k+1}\binom{n}{k-1}_q = \binom{n}{k-1}_q \cdot \frac{(1-q^{n-k+1})+q^{n-k+1}(1-q^k)}{1-q^k} = \binom{n}{k-1}_q \cdot \frac{1-q^{n+1}}{1-q^k} = \binom{n+1}{k}_q$, recovering the off-by-one form. □

Proof of Theorem 23. Induction on n, following the Lean proof `QSeries.prod_one_add_mul_pow_eq_sum_qBinom` in `QSeries/FiniteBinomial.lean`. The case $n = 0$ gives $1 = 1$.

For the inductive step, set $P_n(z) := \prod_{k=0}^{n-1}(1 + zq^k)$ and $Q_n(z) := \sum_{k=0}^{n} q^{\binom{k}{2}}\binom{n}{k}_q z^k$, so the theorem reads $P_n = Q_n$. By `Finset.prod_range_succ` and the inductive hypothesis $P_n = Q_n$,

$$P_{n+1}(z) \;=\; P_n(z)\,(1 + zq^n) \;=\; Q_n(z)\,(1 + zq^n),$$

so it suffices to show $Q_{n+1}(z) = Q_n(z)\,(1 + zq^n)$. We decompose $Q_{n+1}(z) = \sum_{k=0}^{n+1} q^{\binom{k}{2}}\binom{n+1}{k}_q z^k$ in four explicit steps (mirroring `stepB`–`stepD` of the Lean proof).

Step A (peel off $k = 0$ via `Finset.sum_range_succ'`). Using $\binom{n+1}{0}_q = 1$,

$$Q_{n+1}(z) \;=\; 1 \;+\; \sum_{k=0}^{n} q^{\binom{k+1}{2}} \binom{n+1}{k+1}_q z^{k+1}.$$

Step B (q-Pascal split). Apply Lemma 25 inside the sum and split via `Finset.sum_add_distrib`:

$$\sum_{k=0}^{n} q^{\binom{k+1}{2}} \binom{n+1}{k+1}_q z^{k+1} = \underbrace{\sum_{k=0}^{n} q^{\binom{k+1}{2}} \binom{n}{k+1}_q z^{k+1}}_{S_1} + \underbrace{\sum_{k=0}^{n} q^{\binom{k+1}{2}+n-k} \binom{n}{k}_q z^{k+1}}_{S_2}.$$

Step C ($S_2 = zq^n\,Q_n(z)$). The identity $\binom{k+1}{2} = \binom{k}{2} + k$ (helper `choose_two_succ`) and $k+(n-k) = n$ (valid because $k \le n$, by `Nat.sub_add_cancel`) give $q^{\binom{k+1}{2}+n-k}\, z^{k+1} = z\,q^n \cdot q^{\binom{k}{2}}\, z^k$, hence

$$S_2 = z\,q^n \sum_{k=0}^{n} q^{\binom{k}{2}} \binom{n}{k}_q z^k = z\,q^n\,Q_n(z).$$

Step D ($1 + S_1 = Q_n(z)$). Reindex $j = k+1$ to identify $S_1 = \sum_{j=1}^{n+1} q^{\binom{j}{2}} \binom{n}{j}_q z^j$, then adjoin the $j = 0$ term 1 (using `Finset.sum_range_succ'` in reverse):

$$1 + S_1 = \sum_{j=0}^{n+1} q^{\binom{j}{2}} \binom{n}{j}_q z^j.$$

The $j = n+1$ term vanishes by Lemma 30 ($\binom{n}{n+1}_q = 0$), reducing this to $Q_n(z)$.

Combining the four steps, $Q_{n+1}(z) = (1 + S_1) + S_2 = Q_n(z) + zq^n Q_n(z) = Q_n(z)\,(1 + zq^n)$. The final algebraic identity is closed in Lean by `linear_combination`. □

3.3 Passing to the infinite case

Proof of Theorem 24. We follow Heine's classical functional-equation argument, which is the route realised in Lean (`QSeries.hasSum_qPochhammer_div_mul_pow`). Define

$$c_n := \frac{(a;q)_n}{(q;q)_n}, \qquad F(z) := \sum_{n\ge 0} c_n\, z^n, \qquad G(z) := \frac{(az;q)_\infty}{(z;q)_\infty}.$$

The argument has three pieces.

(i) Coefficient recurrence. From $(a;q)_{n+1} = (a;q)_n(1-aq^n)$ and $(q;q)_{n+1} = (q;q)_n(1-q^{n+1})$,

$$c_{n+1}\,(1-q^{n+1}) = c_n\,(1-aq^n).$$

(Note that $|q| < 1$ forces $1 - q^{n+1} \neq 0$, so c_n is well-defined.)

(ii) Functional equation $(1-z)\,H(z) = (1-az)\,H(qz)$ for $H \in \{F, G\}$. For F: expand both sides as power series; the coefficient identity in (i) shows the series of $(1-z)F(z)$ and $(1-az)F(qz)$ agree term-by-term. The sum $F(z)$ converges absolutely on $\|z\| < 1$ because the coefficient sequence c_n is bounded (its numerator $\|(a;q)_n\|$ converges by Lemma 34 and its denominator $\|(q;q)_n\|$ is eventually bounded below by a positive constant). For G: from the telescoping identity $(z;q)_\infty = (1-z)\,(zq;q)_\infty$ (an instance of $\prod_{k\ge 0} f_k = f_0 \cdot \prod_{k\ge 1} f_k$) applied to both $(z;q)_\infty$ and $(az;q)_\infty$.

(iii) Iteration and passage to the limit. Iterating the functional equation n times on the open unit disc gives

$$F(z)\cdot(z;q)_n = F(q^n z)\cdot(az;q)_n$$

for every $n \ge 0$. As $n \to \infty$:

- $(z;q)_n \to (z;q)_\infty$ and $(az;q)_n \to (az;q)_\infty$ by Lemma 34 (the partial products of a multipliable family converge to its `tprod`);
- $F(q^n z) \to F(0) = c_0 = 1$: this is Tannery's theorem (`tendsto_tsum_of_dominated_convergence`) applied summand-by-summand, with the dominating bound $\|c_k (q^n z)^k\| \le C \|z\|^k$ (summable in k, uniformly in n).

Therefore $F(z) \cdot (z;q)_\infty = (az;q)_\infty$. Since $\|z\| < 1$ implies $(z;q)_\infty \neq 0$ (no factor $1 - zq^k$ can be zero, by the norm estimate; combined with multipliability this gives non-vanishing of the `tprod`), we may divide to conclude $F(z) = G(z)$. □

Remark (alternative route). A different classical route passes $n \to \infty$ in a Cauchy-type *finite* analog

$$\sum_{k=0}^{n} \binom{n}{k}_q \frac{(a;q)_k}{(q;q)_k} z^k \xrightarrow{n\to\infty} \sum_{k=0}^{\infty} \frac{(a;q)_k}{(q;q)_k} z^k,$$

using $(q;q)_k/(q;q)_n \to 1/(q^{k+1};q)_\infty$ and dominated convergence. The Heine route used above avoids the bookkeeping of a separate finite identity and is the one matched by the Lean formalisation.

Avoiding the infinite version entirely. For Jacobi's triple product via Zhu's semi-finite proof, you do not actually need Theorem 24. You only need the *first Euler identity*

$$(-z;q)_\infty = \sum_{n=0}^{\infty} \frac{q^{\binom{n}{2}}}{(q;q)_n} z^n,$$

which is the $n \to \infty$ limit of Theorem 23 after rewriting $\prod_{k=0}^{n-1}(1 + zq^k)$ as $(-z;q)_n$ and dividing by suitable factors. This limit is gentler than the full Cauchy identity.

4 The q-Pochhammer symbol and Gaussian binomial coefficient (formalized)

This section records the foundational definitions and lemmas that have been formalized in Lean for the q-series approach to Jacobi's triple product. The corresponding source files are in `QSeries/` in the `QSeries` Lean library, under the namespace `QSeries`. Throughout this section R is a commutative ring and $a, q \in R$.

4.1 The q-Pochhammer symbol

Definition 26 (Finite q-Pochhammer symbol)**.** For $n \in \mathbb{N}$, the finite q-Pochhammer symbol is

$$(a;q)_n := \prod_{k=0}^{n-1} (1 - a\,q^k).$$

In Lean, this is implemented as `∏ k ∈ Finset.range n, (1 - a * q^k)`, specialising to $(a;q)_0 = 1$ (the empty product).

Lemma 27 (Base case)**.** $(a;q)_0 = 1$.

Proof. The empty product is 1 (`Finset.prod_range_zero`). □

Lemma 28 (Recurrence)**.** *For all $n \in \mathbb{N}$,*

$$(a;q)_{n+1} \;=\; (a;q)_n \cdot (1 - a\,q^n).$$

Proof. Immediate from `Finset.prod_range_succ`. □

4.2 The Gaussian binomial coefficient

Definition 29 (Gaussian binomial coefficient)**.** The Gaussian binomial coefficient $\binom{n}{k}_q \in R$ is defined by recursion on n and k:

$$\binom{0}{0}_q = 1, \quad \binom{0}{k+1}_q = 0,$$
$$\binom{n+1}{0}_q = 1, \quad \binom{n+1}{k+1}_q = \binom{n}{k+1}_q + q^{n-k}\binom{n}{k}_q.$$

This is the q-Pascal recurrence in the form stated in Lemma 25 (with the index shift $k \mapsto k+1$). By construction $\binom{n}{k}_q$ is a polynomial in q with integer coefficients, defined for every pair $(n,k) \in \mathbb{N}^2$ (no division, no roots-of-unity exclusion).

Lemma 30 (Vanishing above the diagonal)**.** *If $n < k$, then $\binom{n}{k}_q = 0$.*

Proof. Induction on n and k following the four-case recursive definition. The non-trivial case is $(n+1, k+1)$ with $n < k$: the recurrence gives $\binom{n+1}{k+1}_q = \binom{n}{k+1}_q + q^{n-k}\binom{n}{k}_q$, and both inductive hypotheses (at $(n, k+1)$ and (n,k), available because $n < k+1$ and $n < k$ respectively) yield 0. □

Lemma 31 (Diagonal)**.** $\binom{n}{n}_q = 1$ *for every $n \in \mathbb{N}$.*

Proof. Induction on n. The case $n = 0$ is by definition. For the step,

$$\binom{n+1}{n+1}_q = \binom{n}{n+1}_q + q^{n-n}\binom{n}{n}_q = 0 + 1 \cdot 1 = 1,$$

using Lemma 30 for the first term and the inductive hypothesis for the second. □

Lemma 32 (Closed form for $\binom{n}{k}_q$)**.** *For all $k \le n$,*

$$\binom{n}{k}_q \cdot (q;q)_k \cdot (q;q)_{n-k} \;=\; (q;q)_n.$$

Proof. Induction on n.

Base case $n = 0$. Forces $k = 0$ and the identity is $1 \cdot 1 \cdot 1 = 1$.

Boundary $k = 0$. Reduces to $1 \cdot 1 \cdot (q;q)_n = (q;q)_n$.

Boundary $k = n+1$. By Lemma 31 we have $\binom{n+1}{n+1}_q = 1$, and $(q;q)_0 = 1$, so both sides equal $(q;q)_{n+1}$.

Inductive step $k+1 \le n$. Apply the q-Pascal recurrence

$$\binom{n+1}{k+1}_q = \binom{n}{k+1}_q + q^{n-k}\binom{n}{k}_q$$

and the factorisations

$$(q;q)_{n-k} \;=\; (q;q)_{n-(k+1)} \cdot (1 - q\,q^{n-(k+1)}), \qquad (q;q)_{k+1} \;=\; (q;q)_k \cdot (1 - q\,q^k),$$

together with the power identities $q \cdot q^{n-(k+1)} = q^{n-k}$ and $q^{n-k} \cdot (q \cdot q^k) = q \cdot q^n$, which use $k \le n$ via `Nat.sub_add_cancel`. The two inductive hypotheses at $(n, k+1)$ and (n, k) then combine into the required identity, dispatched in Lean by `linear_combination`. □

4.3 The finite q-binomial theorem (step 5)

Theorem 23 is formalised as `QSeries.prod_one_add_mul_pow_eq_sum_qBinom` in `QSeries/FiniteBinomial.lean` (in `Qseries_Aristotle_new`). The Lean proof follows exactly the four-step strategy spelled out in the proof attached to Theorem 23 above: peel off $k = 0$, apply the q-Pascal recurrence (Lemma 25) inside the sum, simplify the second piece to $zq^n\,Q_n$, and recombine the first piece via $\binom{n}{n+1}_q = 0$ (Lemma 30).

4.4 The infinite q-Pochhammer symbol and Cauchy identity (steps 6, 8)

Working in $\mathbb{C}$ for the analytic part of the development.

Definition 33 (Infinite q-Pochhammer symbol)**.**

$$(a;q)_\infty \;:=\; \prod_{k=0}^{\infty} (1 - a\,q^k) \;\in\; \mathbb{C},$$

defined unconditionally via `tprod`. The value is mathematically meaningful (and the product is convergent) under the hypothesis $\|q\| < 1$ provided by Lemma 34.

Lemma 34 (Multipliability)**.** *For $a, q \in \mathbb{C}$ with $\|q\| < 1$, the family $k \mapsto 1 - a\,q^k$ is multipliable; in particular the partial products converge to $(a;q)_\infty$.*

Proof. Reduce multipliability to summability of $\sum_k \|aq^k\|$ via Mathlib's `multipliable_one_add_of_summable` (which works in any complete normed ring), then bound $\|aq^k\| = \|a\|\,\|q\|^k$ and conclude by the geometric series $\sum_k \|q\|^k < \infty$ (`summable_geometric_of_lt_one`). □

Theorem 35 (Infinite q-binomial / Cauchy identity, restated for the formal development)**.** *For $a, z, q \in \mathbb{C}$ with $\|q\| < 1$ and $\|z\| < 1$,*

$$\sum_{n=0}^{\infty} \frac{(a;q)_n}{(q;q)_n}\, z^n = \frac{(az;q)_\infty}{(z;q)_\infty}.$$

(Equivalent to Theorem 24.) The Lean theorem is `QSeries.hasSum_qPochhammer_div_mul_pow` in `QSeries/CauchyIdentity.lean` (in `Qseries_Aristotle_new`). The proof realised in Lean follows Heine's functional-equation argument spelled out in the proof of Theorem 24 above, organised under `section CauchyIdentity`: non-vanishing of $(z;q)_\infty$ (`qPochhammerInf_z_q_ne_zero`), the telescoping recursion $(z;q)_\infty = (1-z)\,(zq;q)_\infty$ (`qPochhammerInf_recursion`), the coefficient recurrence $c_{n+1}(1-q^{n+1}) = c_n(1-aq^n)$ (`cauchyCoeff_succ_mul`), the functional equations for F and G (`cauchy_functional_eq_F`, `cauchy_functional_eq_G`), iteration on the disc (`iterated_functional_eq_disc`), and the Tannery-based limit $F(q^n z) \to 1$ (`tendsto_F_qpow`). The alternative route via a finite Cauchy-type analog of Theorem 23 is not formalised.

Remark. Together with Lemma 28, Lemma 30, and Lemma 32, Theorem 23 realises steps 1, 2, 3, 4, and 5 of the formalisation roadmap in Section 3 ("Formalization plan in Lean"). Step 6 is realised by Definition 33 and Lemma 34. Step 8 (the full Cauchy identity, Theorem 24) is now formalised in full via Heine's functional-equation route (`QSeries.hasSum_qPochhammer_div_mul_pow`). Step 3 is partially completed: the recursive definition is in place (Definition 29) and the closed-form bridge to the quotient description is established (Lemma 32); the symmetry identity $\binom{n}{k}_q = \binom{n}{n-k}_q$ remains as future work, as does step 7 (the first Euler identity).

Update. Steps 7 and 8 are now fully formalised, and the Jacobi triple product and Euler's pentagonal number theorem are proved with no `sorry`. The route actually taken by the formalisation diverges from all three textbook sketches above; the analytic proof is documented in Section 5 (including an extension to all $z \neq 0$ in Section 5.8), and a second, independent algebraic proof working entirely in formal power series rings is documented in Section 6.

5 Implemented proof strategy

This section records the proof strategy that was *actually* carried out in the Lean formalisation (produced with the Aristotle prover). It does not follow verbatim any of the three textbook routes – the Hermite-style coefficient recurrence, the Euler / q-binomial theorem, or complex analysis via quasi-periodicity. It is closest in spirit to the Euler / q-binomial route, but the execution is neither Andrews' nor Zhu's: instead of Zhu's semi-finite truncation or a complex-analytic continuation, the formalisation

1. expands $(q;q)_\infty(-z;q)_\infty$ and $(-q/z;q)_\infty$ by the *second* Euler identity and forms their full Cauchy product on $\mathbb{N} \times \mathbb{N}$;
2. evaluates every diagonal coefficient through the classical *Durfee rectangle identity* $S_k(q) = 1/(q;q)_\infty$, here proved *analytically* by a contraction recurrence on the differences $S_k - S_{k+1}$ rather than by the usual Young-diagram bijection;
3. removes the convergence (annulus) restriction by proving an *extended* second Euler identity valid for *all* $z \in \mathbb{C}$, so the Cauchy-product argument runs directly on the punctured disc; and
4. derives Euler's pentagonal number theorem from the triple product by the substitution $q \mapsto q^3$, $z \mapsto -q$.

Source files. The development lives in the Lean library `Qseries_Aristotle_new`, split into the modules `QSeries/Defs.lean`, `QSeries/FiniteBinomial.lean`, `QSeries/InfPochhammer.lean`, `QSeries/CauchyIdentity.lean`, `QSeries/EulerIdentities.lean`, `QSeries/JTP_KeyIdentity.lean`, `QSeries/JTP_Core.lean`, `QSeries/JTP_Helpers.lean`, `QSeries/JacobiTripleProduct.lean`, `QSeries/PentagonalNumber.lean`, and `QSeries/JTP_Analytic.lean` (which extends the identity to all $z \neq 0$), all under the namespace `QSeries`. An independent purely algebraic proof of the triple product in the formal power series ring $R[\![X]\!]$ lives in `QSeries/FPS.lean`, `QSeries/FPS_Euler.lean`, and `QSeries/FPS_Algebra.lean` under the namespace `QSeries.FormalPowerSeries`; this is documented in Section 6. The q-Pochhammer / q-binomial foundations (Section 4) are shared between both developments.

5.1 The two Euler identities

Both Euler q-exponential identities are obtained as specialisations of the Cauchy identity (Theorem 35) and the finite q-binomial theorem (Theorem 23).

Lemma 36 (First Euler identity)**.** *For $\|q\| < 1$ and $\|z\| < 1$,*

$$\sum_{n=0}^{\infty} \frac{z^n}{(q;q)_n} = \frac{1}{(z;q)_\infty}.$$

Proof. Specialise the Cauchy identity (Theorem 35) at $a = 0$, using $(0;q)_n = 1$ and $(0 \cdot z;q)_\infty = 1$. □

Lemma 37 (Second Euler identity)**.** *For $\|q\| < 1$ and $\|z\| < 1$,*

$$\sum_{n=0}^{\infty} \frac{q^{\binom{n}{2}} z^n}{(q;q)_n} = (-z;q)_\infty.$$

Proof. Take $N \to \infty$ in the finite q-binomial theorem (Theorem 23), rewriting $\prod_{k=0}^{N-1}(1+zq^k) \to (-z;q)_\infty$ by Lemma 34 and replacing $\binom{N}{k}_q$ by $(q;q)_N/((q;q)_k(q;q)_{N-k})$ (Lemma 32). The exchange of limit and sum is `tendsto_tsum_of_dominated_convergence`, with the dominating bound coming from $(q;q)_N/(q;q)_{N-k} \to 1$ being bounded uniformly in N. Summability of the target series is `QSeries.summable_euler_second`. □

5.2 Expanding the product as a single series

The two factors $(q;q)_\infty(-z;q)_\infty$ are folded into one series using a telescoping identity for the infinite q-Pochhammer symbol.

Lemma 38 (Telescoping)**.** *For $\|q\| < 1$ and every n,*

$$(q;q)_\infty \;=\; (q;q)_n \cdot (q^{n+1};q)_\infty.$$

Proof. Induction on n, using $(q;q)_{n+1} = (q;q)_n(1-q^{n+1})$ (Lemma 28) and the recursion $(z;q)_\infty = (1-z)(zq;q)_\infty$ (`QSeries.qPochhammerInf_eq_one_sub_mul`). □

Lemma 39 (Product as a series)**.** *For $\|q\| < 1$ and $\|z\| < 1$,*

$$\sum_{n=0}^{\infty} q^{\binom{n}{2}} z^n \,(q^{n+1};q)_\infty = (q;q)_\infty \,(-z;q)_\infty.$$

Proof. Multiply the second Euler identity (Lemma 37) by the constant $(q;q)_\infty$ and rewrite $(q;q)_\infty/(q;q)_n = (q^{n+1};q)_\infty$ via Lemma 38. □

5.3 The key identity $S_k = 1/(q;q)_\infty$

This is the core of the formalisation, replacing both the coefficient-recurrence bookkeeping of Proof 1 and the complex analysis of Proof 3. After the Cauchy product is rearranged by diagonals, each diagonal coefficient is exactly one of the sums

$$S_k(q) \;:=\; \sum_{m=0}^{\infty} \frac{q^{\,m(m+k)}}{(q;q)_m\,(q;q)_{m+k}},$$

and all of them collapse to $1/(q;q)_\infty$. This is the classical *Durfee rectangle identity*: combinatorially, $m \times (m+k)$ is the Durfee rectangle of a partition, contributing $q^{m(m+k)}$, with the regions to its right and below contributing $1/(q;q)_m$ and $1/(q;q)_{m+k}$; the $k = 0$ case is the classical Durfee square identity. (See Andrews, *The Theory of Partitions*, 1976, and Gessel, *Some generalized Durfee square identities*, Discrete Math. **50** (1984).) What is specific to this formalisation is the proof: rather than the Young-diagram bijection, the identity is established *analytically* through the contraction recurrence below, which is convenient to formalise in Lean.

Definition 40 (The key sum)**.** For $\|q\| < 1$ and $k \in \mathbb{N}$, $S_k(q) := \sum_{m\geq 0} q^{m(m+k)}/((q;q)_m\,(q;q)_{m+k})$.

Lemma 41 (Summability of S_k)**.** *For $\|q\| < 1$, the summand of S_k is summable.*

Proof. The denominators $(q;q)_m(q;q)_{m+k}$ are bounded below in norm by a positive constant (the partial products of a convergent infinite product with nonzero limit), so the summand is dominated by $C\,\|q\|^{m^2}$, which is summable. □

Lemma 42 (Limit of S_k)**.** *For $\|q\| < 1$, $S_k(q) \to 1/(q;q)_\infty$ as $k \to \infty$.*

Proof. The $m = 0$ term is $1/(q;q)_k \to 1/(q;q)_\infty$ (`tendsto_qPochhammer` and non-vanishing of $(q;q)_\infty$). The tail $m \geq 1$ tends to 0 by dominated convergence: each term $q^{m(m+k)}/((q;q)_m(q;q)_{m+k}) \to 0$ as $k \to \infty$, dominated by $\|q\|^{m^2}/C$. □

Lemma 43 (Recurrence for S_k)**.** *For $\|q\| < 1$ and every k,*

$$S_k - S_{k+1} \;=\; q^{\,k+1}\,(S_{k+2} - S_{k+1}).$$

Proof. Combine the two series term-by-term, using $(q;q)_{m+k+1} = (q;q)_{m+k}(1-q^{m+k+1})$ to write $S_k - S_{k+1}$ as a single series, then split the numerator $1 - q^m - q^{m+k+1}$ and reindex the $(1-q^m)$ part by $m \mapsto m+1$. The two pieces reassemble into $q^{k+1}(S_{k+2} - S_{k+1})$. □

Theorem 44 (Key identity)**.** *For $\|q\| < 1$ and every k, $S_k(q) = 1/(q;q)_\infty$.*

Proof. Write $D_k = S_k - S_{k+1}$. Iterating Lemma 43 n times gives $\|D_k\| \leq \|q\|^{\,n(2k+n+1)/2}\,\|D_{k+n}\|$. Since $D_{k+n} \to 0$ (Lemma 42) and $\|q\|^{\cdots} \to 0$, we get $D_k = 0$ for all k. Hence $S_k = S_0$ is constant in k, and its common value equals $\lim_k S_k = 1/(q;q)_\infty$. □

Lemma 45 (Non-negative diagonal coefficient)**.** *For $\|q\| < 1$ and $k \geq 0$,*

$$\sum_{m=0}^{\infty} q^{\binom{m+k}{2}}\,(q^{m+k+1};q)_\infty \cdot \frac{q^{\binom{m}{2}}\,q^m}{(q;q)_m} = q^{\binom{k}{2}}.$$

Proof. Rewrite $(q^{m+k+1};q)_\infty = (q;q)_\infty/(q;q)_{m+k}$ (Lemma 38) and use the arithmetic identity $\binom{m+k}{2}+\binom{m}{2}+m = \binom{k}{2}+m(m+k)$ to reduce the sum to $q^{\binom{k}{2}}\,(q;q)_\infty \cdot S_k(q)$. Apply Theorem 44. □

Lemma 46 (Negative diagonal coefficient)**.** *For $\|q\| < 1$ and $l \geq 0$,*

$$\sum_{n=0}^{\infty} q^{\binom{n}{2}}\,(q^{n+1};q)_\infty \cdot \frac{q^{\binom{n+l+1}{2}}\,q^{n+l+1}}{(q;q)_{n+l+1}} = q^{\binom{l+2}{2}}.$$

Proof. As in Lemma 45, using the companion arithmetic identity $\binom{n}{2} + \binom{n+l+1}{2} + (n+l+1) = \binom{l+2}{2} + n(n+l+1)$ and the key identity $S_{l+1} = 1/(q;q)_\infty$ (Theorem 44). □

5.4 Extended second Euler identity (all z)

To run the Cauchy product on the full punctured disc rather than only the annulus, the second Euler identity is extended to all $z \in \mathbb{C}$.

Lemma 47 (Series recursion). *For $\|q\| < 1$, the series $S(z) := \sum_n q^{\binom{n}{2}} z^n/(q;q)_n$ satisfies $S(z) = (1+z)\,S(qz)$.*

Proof. A term-by-term algebraic identity: the difference of the z- and qz-series equals $z\,S(qz)$, using $(q;q)_n = (q;q)_{n-1}(1-q^n)$. Summability for all z is `QSeries.summable_euler_second'`, proved by the ratio test (the ratio $\|q\|^n\|z\|/\|1-q^{n+1}\| \to 0$). □

Theorem 48 (Extended second Euler identity). *For $\|q\| < 1$ and* every $z \in \mathbb{C}$,

$$\sum_{n=0}^{\infty} \frac{q^{\binom{n}{2}} z^n}{(q;q)_n} = (-z;q)_\infty.$$

Proof. Given any z, choose N with $\|zq^N\| < 1$. Iterating Lemma 47 N times gives $S(z) = \prod_{k=0}^{N-1}(1+zq^k)\cdot S(zq^N)$, and $S(zq^N) = (-zq^N;q)_\infty$ by the (small-argument) second Euler identity (Lemma 37). The product $\prod_{k=0}^{N-1}(1+zq^k)\cdot(-zq^N;q)_\infty = (-z;q)_\infty$ by repeated use of `QSeries.qPochhammerInf_eq_one_sub_mul`. □

Lemma 49 (Extended Euler identity at q/z). *For $\|q\| < 1$ and $z \neq 0$ (no annulus condition),*

$$\sum_{m=0}^{\infty} \frac{q^{\binom{m}{2}}\, q^m\, z^{-m}}{(q;q)_m} = (-q/z;q)_\infty.$$

Proof. Apply Theorem 48 at the point q/z (valid for all q/z, hence all $z \neq 0$). □

5.5 The triple product and bilateral series

Definition 50 (Triple product and bilateral series). jacobiProd$(q,z) := (q;q)_\infty\,(-z;q)_\infty\,(-q/z;q)_\infty$, and the bilateral series jacobiBilateral$(q,z) := \sum_{k\geq 0} z^k q^{\binom{k}{2}} + \sum_{m\geq 0} z^{-(m+1)} q^{\binom{m+2}{2}}$ (the non-negative and negative halves of $\sum_{k\in\mathbb{Z}} z^k q^{k(k-1)/2}$).

5.6 The Jacobi triple product

Theorem 51 (Jacobi triple product). *For $\|q\| < 1$, $\|z\| < 1$, $z \neq 0$,* jacobiProd(q,z) = jacobiBilateral(q,z)*; that is,*

$$(q;q)_\infty\,(-z;q)_\infty\,(-q/z;q)_\infty = \sum_{k\geq 0} z^k q^{\binom{k}{2}} + \sum_{m\geq 0} z^{-(m+1)} q^{\binom{m+2}{2}}.$$

Proof. Expand $(q;q)_\infty(-z;q)_\infty$ as a series (Lemma 39) and $(-q/z;q)_\infty$ via the *extended* second Euler identity (Lemma 49), which holds for every $z \neq 0$ with no lower bound on $\|z\|$. Their Cauchy product over $\mathbb{N}\times\mathbb{N}$ is summable (`Summable.mul_norm`), so by `Summable.tsum_prod` the double sum may be reordered. Partition $\mathbb{N}\times\mathbb{N}$ into the diagonals $n \geq m$ (index $k = n-m \geq 0$) and $n < m$ (index $l = m-n-1 \geq 0$). The k-diagonal sum is $z^k q^{\binom{k}{2}}$ by Lemma 45, and the l-diagonal sum is $z^{-(l+1)} q^{\binom{l+2}{2}}$ by Lemma 46. Since the extended identity carries no annulus hypothesis, the argument runs directly on the full punctured disc $0 < \|z\| < 1$, with no separate continuation step. □

Remark (divergence from the outline). Compared with the Euler / q-binomial route: the formalisation uses a *genuine Cauchy product* of two second-Euler expansions, not Zhu's semi-finite truncation; the diagonal coefficients are evaluated through the classical Durfee rectangle identity (Theorem 44), but via its analytic contraction-recurrence proof rather than the usual Young-diagram bijection; and the argument is carried out directly on the whole punctured disc by strengthening the Euler identity to all z (Theorem 48), so it needs neither an annulus restriction with a separate extension step, the Liouville-type complex analysis of Proof 3, nor the coefficient bookkeeping of Proof 1. (Using Durfee rectangles to reach the Jacobi triple product is itself known; see W. Chu, *Durfee rectangles and the Jacobi triple product identity*, Acta Math. Sinica **9** (1993), 24–26.)

5.7 Euler's pentagonal number theorem

Definition 52 (Generalized pentagonal number)**.** $\omega(k) := (k(3k-1)/2)$ for $k \in \mathbb{Z}$ (the product $k(3k-1)$ is always even), realised in Lean as a natural number.

Theorem 53 (Euler's pentagonal number theorem)**.** *For* $\|q\| < 1$,

$$(q;q)_\infty = \sum_{k\geq 0}(-1)^k q^{\omega(k)} + \sum_{k\geq 0}(-1)^{k+1} q^{\omega(-(k+1))} \;=\; 1 - q - q^2 + q^5 + q^7 - q^{12} - \cdots.$$

Proof. Apply the Jacobi triple product (Theorem 51) with $q \mapsto q^3$ and $z \mapsto -q$; the hypotheses reduce to $\|-q\| < 1$ and $-q \neq 0$, both immediate for $0 < \|q\| < 1$ (the case $q = 0$ is trivial). The left-hand side $(q^3;q^3)_\infty (q;q^3)_\infty (q^2;q^3)_\infty$ is regrouped into $(q;q)_\infty$ by splitting the product $\prod_{n\geq 1}(1-q^n)$ into the three residue classes $\{3k+1\}, \{3k+2\}, \{3k+3\}$ modulo 3. Matching the right-hand exponents k^2 (with sign $(-1)^k$) against $\omega(\pm k)$ gives the pentagonal series. □

5.8 Analytic extension to all $z \neq 0$

Theorem 51 was proved under the restriction $\|z\| < 1$. The module `QSeries/JTP_Analytic.lean` removes this restriction using locally uniform convergence of both sides on $\{z \neq 0\}$ and the functional equation $f(qz) = f(z)/z$ satisfied by both jacobiProd(q, z) and jacobiBilateral(q, z).

Theorem 54 (Summability of bilateral series for all z)**.** *For* $\|q\| < 1$ *and* every $z \in \mathbb{C}$, *the non-negative part* $\sum_{k\geq 0} z^k\, q^{\binom{k}{2}}$ *is summable.*

Proof. The ratio of consecutive terms is $|z|\,|q|^n \to 0$, so the ratio test gives summability; the Weierstrass M-test with $M_k = R^k \|q\|^{\binom{k}{2}}$ (summable by a further ratio test) gives uniform convergence on $|z| \leq R$. □

Theorem 55 (Locally uniform convergence of the product side)**.** *For* $\|q\| < 1$, *the partial products* $\prod_{k<N}(1-q^{2k})(1+zq^{2k-1})(1+q^{2k-1}/z)$ *converge* locally uniformly *on* $\{z \neq 0\}$ *to* jacobiProd(q, z).

Proof. On $\overline{B}(z_0, \|z_0\|/2)$ for any $z_0 \neq 0$: the factor $\prod(1 + (-z)q^k)$ is handled by the uniform convergence of $\prod(1 + a_k)$ on compacta (Weierstrass M-test with $\sum \|a_k\| < \infty$), and the factor $\prod(1 + (-q/z)q^k)$ uses the bound $\| - q/z\| \leq 2\|q\|/\|z_0\|$ on that ball. Products of uniformly convergent bounded sequences converge uniformly. □

Theorem 56 (Locally uniform convergence of the series side)**.** *For* $\|q\| < 1$, *the bilateral partial sums* $\sum_{|k|<N} z^k\, q^{\binom{k}{2}}$ *converge* locally uniformly *on* $\{z \neq 0\}$ *to* jacobiBilateral(q, z).

Proof. The non-negative half is locally uniformly convergent everywhere by Theorem 54 and the M-test. The negative half $\sum_{m\geq 0} z^{-(m+1)} q^{\binom{m+2}{2}}$ is uniformly convergent on $\{\|z^{-1}\| \leq R'\}$; near any $z_0 \neq 0$ the ball $B(z_0, \|z_0\|/2)$ satisfies $\|z^{-1}\| \leq 2/\|z_0\|$. □

Theorem 57 (Analytic Jacobi triple product)**.** *For $\|q\| < 1$ and every $z \neq 0$,*

$$(q;q)_\infty \, (-z;q)_\infty \, (-q/z;q)_\infty = \sum_{k\geq 0} z^k \, q^{\binom{k}{2}} + \sum_{m\geq 0} z^{-(m+1)} \, q^{\binom{m+2}{2}}.$$

Proof. Both sides are locally uniformly convergent on $\{z \neq 0\}$ (Theorems 55 and 56). Both satisfy the functional equation $H(qz) = H(z)/z$ for all $z \neq 0$. For any fixed $z \neq 0$, choose N large enough so that $\|q^N z\| < 1$. Then Theorem 51 (valid at $q^N z$) together with the iterated functional equation for both sides yields equality at z. □

6 Formal power series reformulation (algebraic proof)

This section records the second, independent proof of the Jacobi triple product that was formalised in `Qseries_Aristotle_new/QSeries/FPS.lean`, `QSeries/FPS_Euler.lean`, and `QSeries/FPS_Algebra.lean` under the namespace `QSeries.FormalPowerSeries`. Unlike the analytic proof of Section 5, this proof is *entirely algebraic*: no norms, no $\|q\| < 1$ hypothesis, and no topological analysis beyond the X-adic (pi) topology on $R[\![X]\!]$.

Key idea. The variable q becomes the formal power series indeterminate $X \in R[\![X]\!]$, while z lives in the coefficient ring $A = \texttt{LaurentPolynomial}\,\mathbb{C}$ (with $z = T(1)$, $z^{-1} = T(-1)$). The infinite q-Pochhammer symbol $(a;X)_\infty$ is a well-defined element of $R[\![X]\!]$ because the factors $(1 - aX^k)$ converge to 1 in the pi topology: each factor affects only finitely many coefficients of any fixed degree.

6.1 FPS q-Pochhammer symbols

Throughout this section R is a commutative ring (with `DiscreteTopology`).

Definition 58 (FPS finite q-Pochhammer symbol)**.** For $a \in R[\![X]\!]$ and $n \in \mathbb{N}$,

$$\texttt{qPoch}\, a\, n \;:=\; \prod_{k=0}^{n-1} (1 - a \cdot X^k) \;\in\; R[\![X]\!].$$

Lemma 59 (Base case)**.** $\texttt{qPoch}\, a\, 0 = 1$.

Proof. Empty product. □

Lemma 60 (FPS recurrence)**.** $\texttt{qPoch}\, a\, (n+1) = \texttt{qPoch}\, a\, n \cdot (1 - a \cdot X^n)$.

Proof. Immediate from `Finset.prod_range_succ`. □

Lemma 61 (FPS shift identity)**.** $\texttt{qPoch}\, a\, (n+1) = (1-a) \cdot \texttt{qPoch}\, (aX)\, n$.

Proof. Induction on n using the recurrence. □

Lemma 62 (Coefficient stabilisation)**.** *If $d < n$ then $[X^d]\, \texttt{qPoch}\, a\, (n+1) = [X^d]\, \texttt{qPoch}\, a\, n$.*

Proof. The new factor $(1 - aX^n)$ only affects monomials of degree $\geq n > d$. □

Lemma 63 (Constant coefficient)**.** *The constant term of* $\texttt{qPoch}\,(X : R[\![X]\!])\,n$ *is* 1*.*

Proof. Induction on n; each factor $(1 - X \cdot X^k)$ has constant term 1. □

Theorem 64 (FPS multipliability in pi topology)**.** *The family* $k \mapsto 1 - a \cdot X^k$ *is multipliable in* $R[\![X]\!]$ *(with the pi / X-adic topology).*

Proof. Apply `MvPowerSeries.WithPiTopology.multipliable_one_add_of_tendsto_order_atTop_nhds_top`: the X-adic order of $-(aX^k)$ is $\geq k$ (the factor $-(aX^k)$ is divisible by X^k), so the orders tend to ∞, which is the criterion for multipliability in the pi topology. No norm hypothesis is needed. □

Definition 65 (FPS infinite q-Pochhammer symbol)**.**

$$\texttt{qPochInf}\,a \;:=\; \prod_{k=0}^{\infty}(1 - a \cdot X^k) \;\in\; R[\![X]\!].$$

Lemma 66 (Coefficient formula)**.** $[X^d]\,\texttt{qPochInf}\,a = [X^d]\,\texttt{qPoch}\,a\,(d+1)$*.*

Proof. The partial products stabilise at degree d once $n > d$ (Lemma 62), and converge to $\texttt{qPochInf}\,a$ in the pi topology; continuity of coefficient extraction gives the identity. □

Lemma 67 (FPS recursion)**.** $\texttt{qPochInf}\,a = (1 - a) \cdot \texttt{qPochInf}\,(a \cdot X)$*.*

Proof. Extract the $k = 0$ factor from the infinite product and shift: $\prod_{k\geq 0}(1 - aX^k) = (1 - a) \cdot \prod_{k\geq 0}(1 - aX^{k+1}) = (1 - a) \cdot \texttt{qPochInf}(aX)$. □

Lemma 68 (Iterated telescoping)**.** *For every* $n \in \mathbb{N}$*:* $\texttt{qPochInf}\,a = \texttt{qPoch}\,a\,n \cdot \texttt{qPochInf}\,(a \cdot X^n)$*.*

Proof. Induction on n using Lemma 67. □

Lemma 69 (FPS unit)**.** *If* $1 - [X^0]\,a$ *is a unit of* R*, then* $\texttt{qPochInf}\,a$ *is a unit of* $R[\![X]\!]$*.*

Proof. The constant term of $\texttt{qPochInf}\,a$ equals $1 - [X^0]\,a$ (which is a unit), and a power series with unit constant term is a unit. □

6.2 FPS Euler second identity

Theorem 70 (FPS Euler second identity)**.** *In* $R[\![X]\!]$ *(for any commutative ring* R *with discrete topology),*

$$\texttt{qPochInf}(-a) \;=\; \sum_{k=0}^{\infty} X^{\binom{k}{2}} \cdot a^k \cdot \left(\texttt{qPoch}\,(X : R[\![X]\!])\,k\right)^{-1}.$$

Proof. At each degree d, only finitely many terms contribute (those with $\binom{k}{2} \leq d$, i.e. $k \leq d + 1$). The key algebraic step is: $[X^j]\,\texttt{qBinom}(N, k, X) = [X^j]\,(\texttt{qPoch}(X, k))^{-1}$ whenever $j + k \leq N$ (`coeff_qBinom_eq_qPochInv`). Then the finite q-binomial theorem (Theorem 23 with $z = -a$) gives $\texttt{qPoch}(-a, N) = \sum_{k=0}^{N} X^{\binom{k}{2}}\texttt{qBinom}(N, k, X)(-a)^k$ in $R[\![X]\!]$. Taking $N = d + 1$ and extracting the degree-d coefficient yields the identity at each degree. The sum is summable (each degree has finitely many nonzero contributions) and the tsum specialises to the tprod as $N \to \infty$ in the pi topology. □

6.3 FPS key identity

Definition 71 (FPS key sum)**.** For $k \in \mathbb{N}$, define

$$S_k^{\mathrm{fps}} := \sum_{m=0}^{\infty} X^{m(m+k)} \cdot \big(\texttt{qPoch}(X,m)\big)^{-1} \cdot \big(\texttt{qPoch}(X,m+k)\big)^{-1} \in R[\![X]\!].$$

Lemma 72 (FPS key sum is summable)**.** *The summand of S_k^{fps} is summable in $R[\![X]\!]$.*

Proof. The monomial $X^{m(m+k)}$ has X-adic order $\geq m$; since $m \to \infty$, the summand family satisfies the pi-topology criterion for summability. □

Lemma 73 (FPS key sum recurrence)**.** *For every k:*

$$S_k^{\mathrm{fps}} - S_{k+1}^{\mathrm{fps}} = X^{k+1} \cdot (S_{k+2}^{\mathrm{fps}} - S_{k+1}^{\mathrm{fps}}).$$

Proof. Combine the two series term-by-term. Write $(\texttt{qPoch}(X, m+k))^{-1} = (1 - X^{m+k+1}) \cdot (\texttt{qPoch}(X, m+k+1))^{-1}$ (`qPochInv_succ_mul`), split the numerator, and reindex the $(1-X^m)$-part by $m \mapsto m+1$. This is a *purely algebraic* ring identity in $R[\![X]\!]$; no norms are needed. □

Theorem 74 (FPS: all S_k are equal)**.** $S_k^{\mathrm{fps}} = S_0^{\mathrm{fps}}$ *for all $k \in \mathbb{N}$.*

Proof. Let $D_k = S_k^{\mathrm{fps}} - S_{k+1}^{\mathrm{fps}}$. By Lemma 73, $D_k = X^{k+1} D_{k+2} + X^{k+1} D_{k+1}$; iterating, $[X^d]\, D_k = 0$ for all $d < k+1$ (directly from the recurrence, since $[X^d]\, X^{k+1} = 0$ when $d < k+1$). For $d \geq k+1$, induction on d using the recurrence (strong induction) yields $[X^d]\, D_k = 0$ as well, because the only contributing term $[X^{k+1}]X^{k+1} = 1$ forces $[X^{d-(k+1)}]\, D_{k+2} = [X^{d-(k+1)}]\, D_k$ and the argument closes by strong induction. Hence $D_k = 0$ for all k, giving $S_k^{\mathrm{fps}} = S_0^{\mathrm{fps}}$. □

Theorem 75 (FPS key identity)**.** *For every k,*

$$S_k^{\mathrm{fps}} = \big(\texttt{qPochInf}(X)\big)^{-1} =: \texttt{qqInv}.$$

Proof. By Theorem 74, $S_k^{\mathrm{fps}} = S_{d+1}^{\mathrm{fps}}$ for any d. For $k = d+1 > d$, the only term contributing to $[X^d]\, S_{d+1}^{\mathrm{fps}}$ is $m = 0$ (the X^0 monomial), giving $[X^d]\, (\texttt{qPoch}(X, d+1))^{-1}$. For $d+1$ steps of the recursion $\texttt{qPochInf} = \texttt{qPoch}(X,n) \cdot \texttt{qPochInf}(X \cdot X^n)$, one shows $[X^d]\, (\texttt{qPoch}(X,k))^{-1} = [X^d]\, \texttt{qqInv}$ for $d < k$ (Lemma `coeff_qPochInv_eq_qqInv`). Hence $[X^d]\, S_k^{\mathrm{fps}} = [X^d]\, \texttt{qqInv}$ for all d. □

Comparison with the analytic key identity. The analytic key identity (Theorem 44) proves $S_k = 1/(q;q)_\infty$ using a *norm estimate*: $\|D_k\| \leq \|q\|^{n(2k+n+1)/2} \|D_{k+n}\| \to 0$. The FPS key identity (Theorem 75) proves the same identity *coefficient by coefficient* using only ring arithmetic in $R[\![X]\!]$, requiring no analytic hypotheses whatsoever.

6.4 FPS Cauchy coefficient identities

Lemma 76 (FPS product expansion)**.** *In $R[\![X]\!]$:*

$$\texttt{qPochInf}(X) \cdot \texttt{qPochInf}(-a) = \sum_{n=0}^{\infty} X^{\binom{n}{2}}\, a^n\, \texttt{qPochInf}(X \cdot X^n).$$

Proof. Expand $\texttt{qPochInf}(-a)$ via Theorem 70 and distribute $\texttt{qPochInf}(X)$ through the tsum. The identity $\texttt{qPochInf}(X) \cdot (\texttt{qPoch}(X, n))^{-1} = \texttt{qPochInf}(X \cdot X^n)$ (Lemma 68) converts each term. □

Theorem 77 (FPS Cauchy coefficient – non-negative diagonal)**.** *For every $k \geq 0$:*

$$\sum_{m=0}^{\infty} [X^{(m+k).\mathit{choose}\,2} \cdot \mathit{qPochInf}(X \cdot X^{m+k})] \cdot [X^{m.\mathit{choose}\,2} \cdot X^m \cdot (\mathit{qPoch}(X, m))^{-1}] \;=\; X^{k.\mathit{choose}\,2}.$$

That is, the k-th diagonal sum of the Cauchy product equals $X^{\binom{k}{2}}$.

Proof. The diagonal sum equals $X^{\binom{k}{2}} \cdot \texttt{qPochInf}(X) \cdot S_k^{\mathrm{fps}}$ after applying the arithmetic identity $\binom{m+k}{2} + \binom{m}{2} + m = \binom{k}{2} + m(m+k)$ (`choose2_add`) and Lemma 68. Apply Theorem 75 and $\texttt{qPochInf}(X) \cdot \texttt{qqInv} = 1$. □

Theorem 78 (FPS Cauchy coefficient – negative diagonal)**.** *For every $l \geq 0$:*

$$\sum_{n=0}^{\infty} [X^{n.\mathit{choose}\,2} \cdot \mathit{qPochInf}(X \cdot X^n)] \cdot [X^{(n+l+1).\mathit{choose}\,2} \cdot X^{n+l+1} \cdot (\mathit{qPoch}(X, n+l+1))^{-1}] \;=\; X^{(l+2).\mathit{choose}\,2}.$$

Proof. Analogous to Theorem 77, using the companion arithmetic identity $\binom{n}{2} + \binom{n+l+1}{2} + (n + l + 1) = \binom{l+2}{2} + n(n+l+1)$ (`choose2_add'`) and $S_{l+1}^{\mathrm{fps}} = \texttt{qqInv}$. □

6.5 FPS Jacobi triple product

Definition 79 (FPS JTP objects)**.** Let $A = \texttt{LaurentPolynomial}\,\mathbb{C}$, $z = T(1)$, $z^{-1} = T(-1)$ viewed as constant power series in $A[\![X]\!]$. Define:

$$\begin{aligned} \texttt{jtpProd} &:= \texttt{qPochInf}(X) \cdot \texttt{qPochInf}(-z) \cdot \texttt{qPochInf}(-X \cdot z^{-1}) \;\in\; A[\![X]\!], \\ \texttt{jtpSeries} &:= \Big(\sum_{n \geq 0} T(n) \cdot X^{n.\mathrm{choose}\,2}\Big) + \Big(\sum_{m \geq 0} T(-(m+1)) \cdot X^{(m+2).\mathrm{choose}\,2}\Big) \;\in\; A[\![X]\!]. \end{aligned}$$

Here $T(k)$ is the degree-k monomial in the Laurent polynomial ring A, so $T(n) = z^n$ and $T(-(m+1)) = z^{-(m+1)}$.

Theorem 80 (FPS Jacobi triple product)**.** *In $A[\![X]\!]$ (with $A = \mathit{LaurentPolynomial}\,\mathbb{C}$):*

$$\mathit{jtpProd} \;=\; \mathit{jtpSeries},$$

that is,

$$\mathit{qPochInf}(X) \cdot \mathit{qPochInf}(-z) \cdot \mathit{qPochInf}(-X/z) \;=\; \sum_{k \geq 0} z^k X^{\binom{k}{2}} \;+\; \sum_{m \geq 0} z^{-(m+1)} X^{\binom{m+2}{2}}.$$

Proof. Expand `jtpProd` using Lemma 76 (on the $\texttt{qPochInf}(X) \cdot \texttt{qPochInf}(-z)$ factor) and Theorem 70 (on $\texttt{qPochInf}(-Xz^{-1})$), forming a double tsum over $\mathbb{N} \times \mathbb{N}$. Summability of the double product $a_n \cdot b_m$ (where $a_n = X^{\binom{n}{2}} z^n \texttt{qPochInf}(X \cdot X^n)$ and $b_m = X^{\binom{m}{2}+m} z^{-m} (\texttt{qPoch}(X, m))^{-1}$) follows from the pi-topology structure: each coefficient of $a_n \cdot b_m$ is eventually zero in n (once $\binom{n}{2} > d$) and in m (once $\binom{m}{2} + m > d$).

Partition $\mathbb{N} \times \mathbb{N}$ via the bijection $\texttt{diagEquiv} : (n, m) \mapsto \mathrm{inl}(n-m, m)$ if $m \leq n$, $\mathrm{inr}(m-n-1, n)$ otherwise. The k-diagonal ($m \leq n, k = n-m$) sum equals $z^k X^{\binom{k}{2}}$ by Theorem 77; the l-diagonal ($m > n, l = m-n-1$) sum equals $z^{-(l+1)} X^{\binom{l+2}{2}}$ by Theorem 78. Summing over all k and l gives `jtpSeries`. □

Comparison with Section 5.

- The FPS proof (Theorem 80) works over *any* commutative ring with discrete topology and needs no $\|q\| < 1$ hypothesis; the analytic proof (Theorem 51) works in $\mathbb{C}$ with $\|q\| < 1$ and $\|z\| < 1$.
- The analytic proof is extended to all $z \neq 0$ by Theorem 57; the FPS proof is already valid for all $z \in A^\times$.
- Both use the same algebraic infrastructure (Sections 4–4.3). The key identity ($S_k = (q;q)_\infty^{-1}$) is proved analytically in Theorem 44 and algebraically (in $R[\![X]\!]$) in Theorem 75.