1. The Jacobi Triple Product Identity

These are notes on the Jacobi Triple Product Identity and its use in proving the Euler Pentagonal Number Theorem and the mod 5 and 7 congruences for the partition number. I have included in a few more of the details than I included in the lectures.

Let $P$ be the set of all partitions and let $D_n$ be the set of all partitions of $n$ into distinct parts only. Let $T_k$ denote the partition $(k, k-1, \ldots, 1)$.

Lemma 1.1. [Sylvester’s Decomposition]

$$P \times \{T_k\} \cong \bigcup_{j \geq 0} D_{k+j} \times (D_j \cup D_{j-1})$$

where $D_0 \cup D_{-1} = D_0$.

Proof. Append the reverse $(1, 2, \ldots, k)$ of $T_k$ to the top of the Ferrers diagram for $\pi \in P$, and consider the staircase that continues the profile of the Ferrers diagram for $\pi$. The length of the staircase is $k+j$. The staircase partitions the diagram into a partition $\alpha$ obtained by summing the columns of $\star$’s below the staircase, and a partition $\beta$ obtained by summing the $\star$’s in rows above the staircase. The number of rows in $\beta$ is $j$ or $j-1$. The partitions $\alpha$ and $\beta$ necessarily have distinct parts, induced by the staircase. The construction is clearly reversible.

Theorem 1.2. [Jacobi Triple Product Identity]

$$\prod_{m \geq 1} \left(1 - q^{2m}\right) \left(1 + yq^{2m-1}\right) \left(1 + y^{-1}q^{2m-1}\right) = \sum_{k=-\infty}^{\infty} y^k q^{k^2}.$$
Proof. From Lemma 1.1, by counting partitions with respect to the sum of their parts, marked by $\text{Proof.}$, we have
\[
q^{(k+1)} \prod_{m \geq 1} (1 - q^m)^{-1} = \sum_{j \geq 0} [s^{k+j}] \prod_{a \geq 1} (1 + sq^a)
\]
\[
\cdot \left[ (j) \prod_{b \geq 1} (1 + t q^b) + [j^{-1}] \prod_{b \geq 1} (1 + t q^b) \right]
\]
\[
= \sum_{j \geq 0} [s^{k+j}] (1 + t) \prod_{m \geq 1} (1 + sq^m) (1 + t q^m)
\]
\[
= \sum_{j \geq 0} [s^{k+j}] \prod_{m \geq 1} (1 + sq^m) (1 + t q^{m-1}).
\]
We now change variables from $s$ and $t$ to $s$ and $u$ through $st = u$. Then
\[
q^{(k+1)} \prod_{m \geq 1} (1 - q^m)^{-1} = [s^k] \prod_{m \geq 1} (1 + sq^m) (1 + s^{-1}q^{m-1}).
\]
so
\[
(1.1) \quad q^{(k+1)} \prod_{m \geq 1} (1 - q^m)^{-1} = [s^k] \prod_{m \geq 1} (1 + sq^m) (1 + s^{-1}q^{m-1}).
\]
We next sum over $k$ from $-\infty$ to $+\infty$ by making use of the following symmetry in $k$. Replacing $s$ by $s^{-1}$, we have
\[
q^{(k+1)} \prod_{m \geq 1} (1 - q^m)^{-1} = [s^{-k}] \prod_{m \geq 1} (1 + s^{-1}q^m) (1 + sq^{m-1}).
\]
Now replace $s$ by $qS$, noting that $[s^{-k}] = q^k [S^{-k}]$. Then
\[
q^{(k+1)} \prod_{m \geq 1} (1 - q^m)^{-1} = q^k [S^{-k}] \prod_{m \geq 1} (1 + S^{-1}q^{m-1}) (1 + Sq^m)
\]
so, replacing $S$ by $s$,
\[
q^{(k+1)} \prod_{m \geq 1} (1 - q^m)^{-1} = [s^{-k}] \prod_{m \geq 1} (1 + sq^m) (1 + s^{-1}q^{m-1})
\]
since $\binom{k+1}{2} - k = \binom{-k+1}{2}$. Thus (1.1) holds with $k$ replaced by $-k$. Thus summing (1.1) over $k$ from $-\infty$ to $+\infty$ we have
\[
\sum_{k=-\infty}^{\infty} s^k q^{(k+1)} \prod_{m \geq 1} (1 - q^m)^{-1} = \sum_{k=-\infty}^{\infty} s^k [s^k] \prod_{m \geq 1} (1 + sq^m) (1 + s^{-1}q^{m-1})
\]
\[
= \prod_{m \geq 1} (1 + sq^m) (1 + s^{-1}q^{m-1})
\]
so
\[
\sum_{k=-\infty}^{\infty} s^k q^{(k+1)} = \prod_{m \geq 1} (1 - q^m) (1 + sq^m) (1 + s^{-1}q^{m-1}).
\]
Replacing $q$ by $q^2$,
\[
\sum_{k=-\infty}^{\infty} s^k q^{k(k+1)} = \prod_{m \geq 1} (1 - q^{2m}) (1 + sq^{2m}) (1 + s^{-1}q^{2m-2}).
\]
Let \( sq = y \). Then
\[
\sum_{k=\infty}^{\infty} y^k q^{k^2} = \prod_{m \geq 1} \left( 1 - q^{2m} \right) \left( 1 + y q^{2m-1} \right) \left( 1 + y^{-1} q^{2m-1} \right),
\]
which completes the proof.

Note that \( \sum_{k=\infty}^{\infty} y^k q^{k^2} \in \mathbb{Q}[y, y^{-1}][q] \), the ring of formal power series in \( q \) with a coefficient ring that is polynomial in \( y \) and \( y^{-1} \).

**Example 1.3.** Find the number of integer points on the \( d \)-sphere of radius \( r \).

The \( d \)-sphere of radius \( r \) is given by
\[
\left\{ (z_1, \ldots, z_d) \in \mathbb{Z}^d : z_1^2 + \cdots + z_d^2 = r^2 \right\}.
\]
Then the number \( c_{r,d} \) of such points is
\[
c_{r,d} = \left| \left\{ (z_1, \ldots, z_d) \in \mathbb{Z}^d : z_1^2 + \cdots + z_d^2 = r^2 \right\} \right| = \left[ x^{r^2} \right] \left( \sum_{k=\infty}^{\infty} x^{k^2} \right)^d.
\]
so, by the Jacobi Triple Product Theorem, with \( y = 1 \), we have
\[
c_{r,d} = \left[ x^{r^2} \right] \prod_{m \geq 1} \left( 1 - x^{-2m} \right)^d \left( 1 + x^{2m-1} \right)^{2d}.
\]
This has reduced the original question from a multivariate one to a univariate one.

The following result is an immediate consequence of the Jacobi Triple Product Identity.

**Theorem 1.4.** [Euler Pentagonal Number Theorem]
\[
\prod_{m \geq 1} (1 - q^m) = \sum_{k=\infty}^{\infty} (-1)^k q^{(3k-1)/2}.
\]

**Proof.** From the Jacobi Triple Product Identity,
\[
\prod_{m \geq 1} \left( 1 - q^{2m} \right) (1 + y q^{2m-1}) (1 + y^{-1} q^{2m-1}) = \sum_{k=\infty}^{\infty} y^k q^{k^2}.
\]
First, replacing \( q \) by \( q^{3/2} \) gives
\[
\prod_{m \geq 1} \left( 1 - q^{3m} \right) \left( 1 + y q^{3m-3/2} \right) \left( 1 + y^{-1} q^{3m-3/2} \right) = \sum_{k=\infty}^{\infty} y^k q^{3k^2/2}.
\]
and then replacing \( y \) by \( -q^{-1/2} \) gives
\[
\prod_{m \geq 1} \left( 1 - q^{3m} \right) \left( 1 - q^{3m-2} \right) (1 + q^{3m-1}) \left( 1 + q^{3m-2} \right) = \sum_{k=\infty}^{\infty} (-1)^k q^{(3k-1)/2}.
\]
The result follows immediately since the exponents on the right hand side give a complete set of residues modulo 3.
The Euler Pentagonal Number Theorem has a combinatorial interpretation in terms of partitions.

**Corollary 1.5.** The number of partitions in \( D_n \) with an even number of parts minus the number of partitions in \( D_n \) with an odd number of parts is equal to \((-1)^k\) if there is an integer \( k \) such that \( n = k(3k - 1)/2 \) and is 0 otherwise.

**Proof.** Let \( d_k(n) \) be the number of partitions in \( D_n \) with \( k \) parts. Then
\[
\sum_{k,n \geq 0} d_k(n)x^kq^n = \prod_{m \geq 1} (1 + xq^m).
\]
Let \( e(n) \) be the number of partitions in \( D_n \) with an even number of parts minus the number of partitions in \( D_n \) with an odd number of parts. Then
\[
e(n) = \sum_{k \geq 0} (-1)^k d_k(n) = \sum_{k \geq 0} (-1)^k [x^k q^n] \prod_{m \geq 1} (1 + xq^m)
\]
\[
= [q^n] \sum_{k \geq 0} (-1)^k [x^k] \prod_{m \geq 1} (1 + xq^m)
\]
\[
= [q^n] \prod_{m \geq 1} (1 - q^m) = [q^n] \sum_{k=-\infty}^{\infty} (-1)^k q^{k(3k-1)/2},
\]
by the Euler Pentagonal Number Theorem. Thus
\[
e(n) = \begin{cases} (-1)^k & \text{if } n = k(3k - 1)/2 \text{ for some integer } k, \\ 0 & \text{otherwise}, \end{cases}
\]
which concludes the proof.

## 2. Congruences for the Partition Number

We begin by proving an expansion theorem.

**Theorem 2.1.**
\[
\prod_{m \geq 1} (1 - q^{2m})^3 = \sum_{k \geq 0} (-1)^k (2k + 1) q^{(k+1)^2}.
\]

**Proof.** In the Jacobi Triple product Identity replace \( y \) by \(-y\) to obtain
\[
\prod_{m \geq 1} (1 - q^{2m}) (1 - yq^{2m-1}) (1 - y^{-1}q^{2m-1}) = \sum_{k=-\infty}^{\infty} (-y)^k q^{k^2}.
\]
But \( \prod_{m \geq 1} (1 - yq^{2m-1}) = (1 - y) \prod_{m \geq 1} (1 - yq^{2m+1}) \) so
\[
(1 - q^{2m}) (1 - y^{-1}q^{2m-1}) (1 - q^{2m}) = (1 - qy)^{-1} \sum_{k=-\infty}^{\infty} (-y)^k q^{k^2}.
\]
Now
\[
(1 - qy)^{-1} \sum_{k=-\infty}^{\infty} (-y)^k q^{k^2} = (1 - qy)^{-1} \left( 1 + \sum_{k=1}^{\infty} \left( (-y)^k + (-y)^{-k} \right) q^{k^2} \right)
\]
\[
= 1 + \sum_{m \geq 1} y^m q^m + \sum_{m \geq 0} y^m \sum_{k=1}^{\infty} \left( (-y)^k + (-y)^{-k} \right) q^{k^2+m}.
\]
Let \( k^2 + m = m' \) and eliminate \( m \) from the summation. Then \( m = m' - k^2 \geq 0 \) so \( k^2 \leq m' \) so \( k \leq \mu_{m'} = \lfloor \sqrt{m'} \rfloor \). Also \( k \geq 1 \) and \( m \geq 0 \) so \( m' \geq 1 \) whence the right hand side of the above expression is equal to \( 1 + \sum_m y^m q^m + \sum_{m'} q^{m'} \sum_{k=1}^{\mu_{m'}} (-y)^k (-y)^{-k} y^{m'-k^2} \) so

\[
(1 - qy)^{-1} \sum_{k=-\infty}^{\infty} (-y)^k q^{k^2} = 1 + \sum_{m \geq 1} q R_m
\]

where \( R_m = \sum_{k=1}^{\mu_m} (-1)^k y^{m-k(k-1)} + \sum_{k=1}^{\mu_{m+1}} (-1)^k y^{m-k(k+1)} \)

\[
R_m = \sum_{k=1}^{\mu_{m+1}} (-1)^{k+1} y^{m-k(k+1)} + \sum_{k=1}^{\mu_m} (-1)^k y^{m-k(k+1)}
\]

so

\[
(1 - qy)^{-1} \sum_{k=-\infty}^{\infty} (-y)^k q^{k^2} = 1 + \sum_{m \geq 1} (-1)^\mu_m y^{m-\mu_m^2 - \mu_m} q^m.
\]

We may therefore set \( y = q^{-1} \) in this expression. This gives

\[
(1 - qy)^{-1} \sum_{k=-\infty}^{\infty} (-y)^k q^{k^2} \bigg|_{y=q^{-1}} = 1 + \sum_{m \geq 1} (-1)^\mu_m y^{m^2 + \mu_m}
\]

\[
= 1 + \sum_{m \geq 1} (-1)^m y^{m^2 + m} \left\{ i \geq 1: \lfloor \sqrt{i} \rfloor = m \right\}
\]

\[
= 1 + \sum_{m \geq 1} (-1)^m (2m + 1) y^{m^2 + m},
\]

since \( \left\{ i \geq 1: \lfloor \sqrt{i} \rfloor = m \right\} = \left\{ i \geq 1: m \leq i \leq (m+1)^2 - 1 \right\} = 2m + 1 \). But

\[
\prod_{m \geq 1} (1 - yq^{2m+1}) (1 - y^{-1}q^{2m-1}) (1 - q^2)_{q=q^{-1}} = \prod_{m \geq 1} (1 - q^{2m})^3
\]

so, from (2.1),

\[
\prod_{m \geq 1} (1 - q^{2m})^3 = 1 + \sum_{m \geq 1} (-1)^m (2m + 1) q^{m^2 + m},
\]

and the result follows by replacing \( q \) by \( q^{1/2} \).

\[
\square
\]

With these results, we may now prove a remarkable congruence for the partition number. The following lemma is needed.
Lemma 2.2. Let $a_0, a_1, \ldots$ be integers, and let $m$ be a non-negative integer not congruent to 0 modulo 5. Then

$$[q^m] (a_0 + a_1 q + a_2 q^2 + \cdots)^5 \equiv 0 \mod 5.$$  

**Proof.** Throughout this proof, $\equiv$ denotes congruence modulo 5. Now

$$[q^m] (a_0 + a_1 q + a_2 q^2 + \cdots)^5 = [q^m] (a_0 + a_1 q + \cdots + a_m q^m)^5 = \sum_{i_0, \ldots, i_m \geq 0} \frac{5!}{i_0! \cdots i_m!} a_{i_0} \cdots a_{i_m}^m,$$

where the sum is over all $i_0, \ldots, i_m$ such that $i_0 + \cdots + i_m = 5$ and $i_1 + 2i_2 + \cdots + mi_m = m$. But $m \not\equiv 0 \mod 5$, so not all of $i_1, 2i_2, \ldots, mi_m$ are congruent to 0 modulo 5. Suppose that $ji_j \not\equiv 0$. Then, in particular, $i_j \not\equiv 0$. But $0 \leq i_j \leq 5$ so $i_j \not= 0$. Thus none of $i_0, \ldots, i_m$ is equal to 5 since their sum is 5. Then

$$\frac{5!}{i_0! \cdots i_m!} \equiv 0.$$

The result follows since $a_{i_0}^i \cdots a_{i_m}^m$ is an integer. \qed

The above lemma is in fact more general, since “5” may be replaced by an arbitrary prime throughout (primality is necessary since, for example, $4!/2!^2$ is not congruent to 0 modulo 4).

**Theorem 2.3.** $p(5n - 1) \equiv 0 \mod 5$.

**Proof.** Throughout this proof, I shall use $\equiv$ to denote congruence modulo 5. Let

$$F(q) = q \prod_{k \geq 1} (1 - q^k)^4.$$  

Then

$$F(q) = q \prod_{i \geq 1} (1 - q^i) \prod_{k \geq 1} (1 - q^k)^3.$$  

From the Euler Pentagonal Number Theorem and Theorem 2.1 we have

$$F(q) = q \sum_{m = -\infty}^{\infty} (-1)^m q^{m(3m-1)/2} \sum_{k \geq 0} (-1)^k (2k + 1) q^{k+1} \frac{1}{k+1}$$

$$= \sum_{m = -\infty}^{\infty} (-1)^{m+k} (2k + 1) q^{1+m(3m-1)/2+\frac{1}{2}k^2}.$$  

Now note that $q \prod_{i \geq 1} (1 - q^i)^{-1} = F(q) \prod_{k \geq 1} (1 - q^k)^{-5}$. Then

$$p(5j - 1) = [q^{5j-1}] \prod_{i \geq 1} (1 - q^i)^{-1} = [q^{5j}] F(q) \prod_{k \geq 1} (1 - q^k)^{-5}$$

so

$$p(5j - 1) = \sum_{n \geq 0} ([q^n] F(q)) \left( [q^{5j-n}] \prod_{k \geq 1} (1 - q^k)^{-5} \right).$$
There are two cases.

**Case 1:** Assume that \( n \equiv 0 \). Then \([q^n] F(q)\) is non-zero if \( 1 + m (3m - 1) / 2 + {k + 1 \choose 2} \equiv n \). Now consider \( 1 + m (3m - 1) / 2 \). If \( m \) is odd, so \( m = 2a + 1 \), then \( 1 + m (3m - 1) / 2 = 1 + m (3a + 1) \equiv 1 + m (-2a + 1) = 1 + m (-m + 2) = -m^2 + 2m + 1 \). If \( m \) is even, so \( m = 2a \), then \( 1 + m (3m - 1) / 2 = 1 + a (6a - 1) \equiv 1 - 4a (a - 1) = 1 - 2m (a - 1) = -m^2 + 2m + 1 \). Thus, for any \( m, 1 + m (3m - 1) / 2 \equiv -m^2 + 2m + 1 \). Then

\[
1 + m (3m - 1) / 2 = -A^2 + 2A + 1 \text{ if } m \equiv A.
\]

Similarly, for \( {k + 1 \choose 2} \), if \( k \) odd then \( k = 2b + 1 \), so \( {k + 1 \choose 2} = k (b + 1) \equiv k (-4b + 1) \equiv k (-2k + 3) \equiv -2k^2 + 3k \equiv 3k^2 - 2k \). If \( k \) is even, so \( k = 2b \), then \( {k + 1 \choose 2} = b (k + 1) \equiv -4b (k + 1) \equiv -2k (k + 1) \equiv 3k^2 - 2k \). Thus, for any \( k, {k + 1 \choose 2} \equiv 3k^2 - 2k \). Then

\[
{k + 1 \choose 2} = 3B^2 - 2B \text{ if } k \equiv B.
\]

By direct computation,

\[
(-A^2 + 2A + 1 \text{ mod } 5: A = 0, \ldots, 4) = (1, 2, 1, 3, 3)
\]

and

\[
(3B^2 - 2B \text{ mod } 5: B = 0, \ldots, 4) = (0, 1, 3, 1, 0).
\]

Then \( 1 + m (3m - 1) / 2 + {k + 1 \choose 2} \equiv 0 \) implies that \( A = 1 \) and \( B = 2 \), since the only two residue classes, one from each of the above two lists, that sum to 0 mod 5 are 2 and 3, which implies that \( m \equiv 1 \) and \( k \equiv 2 \). Thus \( 2k + 1 \equiv 0 \). We conclude that \([q^n] F(q) \equiv 0 \). Thus the contribution to the right hand side of (2.2) is 0 from this case.

**Case 2:** Assume that \( n \not\equiv 0 \). Then neither is \( 5j - n \), so, from Lemma 2.2, \([q^{5j-n}] \prod_{k \geq 1} (1 - q^k)^{−5} \equiv 0 \) since \( (1 - q^k)^{−5} \) is a series with integer coefficients. It follows that the contribution to the right hand side of (2.2) is 0 in this case.

We conclude from (2.2) that \( p(5j - 1) \equiv 0 \), establishing the result. \( \square \)

The following mod 7 congruence may be obtained by a similar argument.

**Theorem 2.4.** \( p(7n - 2) \equiv 0 \mod 7 \).

*Proof.* Throughout this proof, I shall use \( \equiv \) to denote congruence modulo 7. Let

\[
G(q) = q^2 \prod_{i \geq 1} (1 - q^i)^6.
\]

Then

\[
G(q) = q^2 \prod_{i \geq 1} (1 - q^i)^3 \prod_{i \geq k} (1 - q^i)^3.
\]
From Theorem 2.1 we have
\[ G(q) = \sum_{j,k \geq 0} (-1)^{k+j} (2k + 1)(2k+1) q^{2+(j+1)^2+(k+1)^2}. \]

Now note that \( q^2 \prod_{i \geq 1} (1 - q^i)^{-1} = G(q) \prod_{k \geq 1} (1 - q^k)^{-7} \). Then
\[
p(7j - 2) = [q^{7j-2}] (1 - q^i)^{-1} = [q^{7j}] G(q) \prod_{k \geq 1} (1 - q^k)^{-7}
\]
so
\[
(2.3) \quad p(7j - 2) = \sum_{n \geq 0} ([q^n] G(q)) \left( [q^{7j-n}] \prod_{k \geq 1} (1 - q^k)^{-7} \right).
\]

There are two cases.

**Case 1:** Assume that \( n \equiv 0 \). We now proceed as before. It follows easily (the details are omitted) that
\[
2 + \left( \frac{j+1}{2} \right) + \left( \frac{k+1}{2} \right) \equiv (2A + 1)^2 + (2B + 1)^2 \text{ if } j \equiv A \text{ and } k \equiv B.
\]
But by direct computation
\[
((2A + 1) \mod 5: A = 0, \ldots, 4) = (1, 2, 4, 0, 4, 2, 1)
\]
so \( 2 + \left( \frac{j+1}{2} \right) + \left( \frac{k+1}{2} \right) \equiv 0 \) implies that \( A = B = 3 \). Thus \( j = 7J + 3 \) and \( k = 7K + 3 \) for some \( J \) and \( K \), so \( 2j + 1, 2k + 1 \equiv 0 \). We conclude that \( [q^n] G(q) \equiv 0 \). Thus the contribution to the right hand side of (2.3) is 0 from this case.

**Case 2:** Assume that \( n \not\equiv 0 \). Then neither is \( 7j - n \), so, from the comment following Lemma 2.2, \( [q^{7j-n}] \prod_{k \geq 1} (1 - q^k)^{-7} \equiv 0 \) since \( (1 - q^k)^{-7} \) is a series with integer coefficients. It follows that the contribution to the right hand side of (2.3) is 0 in this case.

We conclude from (2.3) that \( p(7j - 2) \equiv 0 \), establishing the result. \(\square\)