NOTES ON THE JACOBI TRIPLE PRODUCT IDENTITY

PROFESSOR D.M.JACKSON

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 $\mathcal{P}$ be the set of all partitions and let $\mathcal{D}_n$ 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]*

$$\mathcal{P} \times \{T_k\} \xrightarrow{\sim} \bigcup_{j \geq 0} \mathcal{D}_{k+j} \times (\mathcal{D}_j \cup \mathcal{D}_{j-1})$$

where $\mathcal{D}_0 \cup \mathcal{D}_{-1} = \mathcal{D}_0$.

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 π. The length of the staircase is $k + j$. The staircase partitions the diagram into a partition α obtained by summing the columns of $\star$'s below the staircase, and a partition β obtained by summing the $\star$'s in rows above the staircase. The number of rows in β is j or $j-1$. The partitions α and β necessarily have distinct parts, induced by the staircase. The construction is clearly reversible. $\square$

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 q, we have

$$\begin{aligned} q^{\binom{k+1}{2}} \prod_{m\geq 1} (1-q^m)^{-1} &= \sum_{j\geq 0} \left[s^{k+j}\right] \prod_{a\geq 1} (1+sq^a) \\ &\quad \cdot \left(\left[t^j\right] \prod_{b\geq 1} \left(1+tq^b\right) + \left[t^{j-1}\right] \prod_{b\geq 1} \left(1+tq^b\right) \right) \\ &= \sum_{j\geq 0} \left[s^{k+j}t^j\right] (1+t) \prod_{m\geq 1} (1+sq^m)(1+tq^m) \\ &= \sum_{j\geq 0} \left[s^{k+j}t^j\right] \prod_{m\geq 1} (1+sq^m)\left(1+tq^{m-1}\right). \end{aligned}$$

We now change variables from s and t to s and u through $st=u$. Then

$$q^{\binom{k+1}{2}} \prod_{m\geq 1} (1-q^m)^{-1} = \left[s^k\right] \sum_{j\geq 0} \left[u^j\right] \prod_{m\geq 1} (1+sq^m)\left(1+us^{-1}q^{m-1}\right)$$

so

$$q^{\binom{k+1}{2}} \prod_{m\geq 1} (1-q^m)^{-1} = \left[s^k\right] \prod_{m\geq 1} (1+sq^m)\left(1+s^{-1}q^{m-1}\right). \tag{1}$$

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

$$q^{\binom{k+1}{2}} \prod_{m\geq 1} (1-q^m)^{-1} = \left[s^{-k}\right] \prod_{m\geq 1} \left(1+s^{-1}q^m\right)\left(1+sq^{m-1}\right).$$

Now replace s by qS, noting that $\left[s^{-k}\right] = q^k \left[S^{-k}\right]$. Then

$$q^{\binom{k+1}{2}} \prod_{m\geq 1} (1-q^m)^{-1} = q^k \left[S^{-k}\right] \prod_{m\geq 1} \left(1+S^{-1}q^{m-1}\right)(1+Sq^m)$$

so, replacing S by s,

$$q^{\binom{-k+1}{2}} \prod_{m\geq 1} (1-q^m)^{-1} = \left[s^{-k}\right] \prod_{m\geq 1} (1+sq^m)\left(1+s^{-1}q^{m-1}\right)$$

since $\binom{k+1}{2} - k = \binom{-k+1}{2}$. Thus (1) holds with k replaced by $-k$. Thus summing (1) over k from $-\infty$ to $+\infty$ we have

$$\begin{aligned} \sum_{k=-\infty}^{\infty} s^k q^{\binom{k+1}{2}} \prod_{m\geq 1} (1-q^m)^{-1} &= \sum_{k=-\infty}^{\infty} s^k \left[s^k\right] \prod_{m\geq 1} (1+sq^m)\left(1+s^{-1}q^{m-1}\right) \\ &= \prod_{m\geq 1} (1+sq^m)\left(1+s^{-1}q^{m-1}\right) \end{aligned}$$

so

$$\sum_{k=-\infty}^{\infty} s^k q^{\binom{k+1}{2}} = \prod_{m\geq 1} (1-q^m)(1+sq^m)\left(1+s^{-1}q^{m-1}\right).$$

Replacing q by q^2,

$$\sum_{k=-\infty}^{\infty} s^k q^{k(k+1)} = \prod_{m\geq 1} \left(1-q^{2m}\right)\left(1+sq^{2m}\right)\left(1+s^{-1}q^{2m-2}\right).$$

Let $sq = y$. Then

$$\sum_{k=-\infty}^{\infty} y^k q^{k^2} = \prod_{m\geq 1} \left(1 - q^{2m}\right)\left(1 + yq^{2m-1}\right)\left(1 + y^{-1}q^{2m-1}\right),$$

which completes the proof. □

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

Example 1.1. *Find the number of integer points on the d-sphere of radius r.*

The d-sphere of radius r is given by

$$\left\{(z_1, \ldots, z_d) \in \mathbb{Z}^d \colon z_1^2 + \cdots + z_d^2 = r^2\right\}.$$

Then the number $c_{r,d}$ of such points is

$$c_{r,d} = \left|\left\{(z_1, \ldots, z_d) \in \mathbb{Z}^d \colon z_1^2 + \cdots + z_d^2 = r^2\right\}\right| = \left[x^{r^2}\right]\left(\sum_{i=-\infty}^{\infty} x^{i^2}\right)^d$$

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 1.3. *[Euler Pentagonal Number Theorem]*

$$\prod_{m\geq 1}\left(1 - q^m\right) = \sum_{k=-\infty}^{\infty} (-1)^k q^{k(3k-1)/2}.$$

Proof. From the Jacobi Triple Product Identity,

$$\prod_{m\geq 1}\left(1 - q^{2m}\right)\left(1 + yq^{2m-1}\right)\left(1 + y^{-1}q^{2m-1}\right) = \sum_{k=-\infty}^{\infty} y^k q^{k^2}.$$

First, replacing q by $q^{3/2}$ gives

$$\prod_{m\geq 1}\left(1 - q^{3m}\right)\left(1 + yq^{3m-3/2}\right)\left(1 + y^{-1}q^{3m-3/2}\right) = \sum_{k=-\infty}^{\infty} y^k q^{3k^2/2}.$$

and then replacing y by $-q^{-1/2}$ gives

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

The result follows immediately since the exponents one 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 1.4. *The number of partitions in* $\mathcal{D}_n$ *with an even number of parts minus the number of partitions in* $\mathcal{D}_n$ *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 $\mathcal{D}_n$ with k parts. Then

$$\sum_{k,n\geq 0} d_k(n)\, x^k q^n = \prod_{m\geq 1}(1+xq^m).$$

Let $e(n)$ be the number of partitions in $\mathcal{D}_n$ with an even number of parts minus the number of partitions in $\mathcal{D}_n$ with an odd number of parts. Then

$$\begin{aligned} e(n) &= \sum_{k\geq 0}(-1)^k d_k(n) = \sum_{k\geq 0}(-1)^k \left[x^k q^n\right]\prod_{m\geq 1}(1+xq^m) \\ &= [q^n]\sum_{k\geq 0}(-1)^k\left[x^k\right]\prod_{m\geq 1}(1+xq^m) \\ &= [q^n]\prod_{m\geq 1}(1-q^m) = [q^n]\sum_{k=-\infty}^{\infty}(-1)^k q^{k(3k-1)/2}, \end{aligned}$$

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.

$$\prod_{m\geq 1}(1-q^m)^3 = \sum_{k\geq 0}(-1)^k(2k+1)\, q^{\binom{k+1}{2}}.$$

Proof. In the Jacobi Triple product Identity replace y by $-y$ to obtain

$$\prod_{m\geq 1}\left(1-q^{2m}\right)\left(1-yq^{2m-1}\right)\left(1-y^{-1}q^{2m-1}\right) = \sum_{k=-\infty}^{\infty}(-y)^k q^{k^2}.$$

But $\prod_{m\geq 1}\left(1-yq^{2m-1}\right) = (1-qy)\prod_{m\geq 1}\left(1-yq^{2m+1}\right)$ so

$$\prod_{m\geq 1}\left(1-yq^{2m+1}\right)\left(1-y^{-1}q^{2m-1}\right)\left(1-q^{2m}\right) = (1-qy)^{-1}\sum_{k=-\infty}^{\infty}(-y)^k q^{k^2}. \tag{2}$$

Now

$$\begin{aligned} (1-qy)^{-1}\sum_{k=-\infty}^{\infty}(-y)^k q^{k^2} &= (1-qy)^{-1}\left(1+\sum_{k=1}^{\infty}\left((-y)^k+(-y)^{-k}\right)q^{k^2}\right) \\ &= 1+\sum_{m\geq 1}y^m q^m + \sum_{m\geq 0}y^m\sum_{k=1}^{\infty}\left((-y)^k+(-y)^{-k}\right)q^{k^2+m}. \end{aligned}$$

Let $k^2+m=m'$ and eliminate m from the summation. Then $m=m'-k^2\geq 0$ so $k^2\leq m'$ so $k\leq\mu_{m'}$ where $\mu_{m'}=\lfloor\sqrt{m'}\rfloor$. Also $k\geq 1$ and $m\geq 0$ so $m'\geq 1$ whence the right hand side of the above expression is equal to $1+\sum_m y^m q^m+\sum_{m'} q^{m'}\sum_{k=1}^{\mu_{m'}}\left((-y)^k+(-y)^{-k}\right)y^{m'-k^2}$ so

$$(1-qy)^{-1}\sum_{k=-\infty}^{\infty}(-y)^k q^{k^2}=1+\sum_{m\geq 1} qR_m$$

where $R_m=\sum_{k=1}^{\mu_m}\left((-y)^k+(-y)^{-k}\right)y^{m-k^2}+y^m$. But

$$\begin{aligned} R_m &= \sum_{k=2}^{\mu_m}(-1)^k y^{m-k(k-1)}+\sum_{k=1}^{\mu_m}(-1)^k y^{m-k(k+1)} \\ &= \sum_{k=1}^{\mu_m-1}(-1)^{k+1} y^{m-k(k+1)}+\sum_{k=1}^{\mu_m}(-1)^k y^{m-k(k+1)} \\ &= (-1)^{\mu_m} y^{m-\mu_m^2-\mu_m}, \end{aligned}$$

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

$$\begin{aligned} (1-qy)^{-1}\sum_{k=-\infty}^{\infty}(-y)^k q^{k^2}\bigg|_{y=q^{-1}} &= 1+\sum_{m\geq 1}(-1)^{\mu_m} y^{\mu_m^2+\mu_m} \\ &= 1+\sum_{m\geq 1}(-1)^m y^{m^2+m}\left|\left\{i\geq 1\colon \lfloor\sqrt{i}\rfloor=m\right\}\right| \\ &= 1+\sum_{m\geq 1}(-1)^m (2m+1)\, y^{m^2+m}, \end{aligned}$$

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

$$\prod_{m\geq 1}\left(1-yq^{2m+1}\right)\left(1-y^{-1}q^{2m-1}\right)\left(1-q^{2m}\right)_{y=q^{-1}}=\prod_{m\geq 1}\left(1-q^{2m}\right)^3$$

so, from (2),

$$\prod_{m\geq 1}\left(1-q^{2m}\right)^3=1+\sum_{m\geq 1}(-1)^m (2m+1)\, q^{m^2+m},$$

and the result follows by replacing q by $q^{1/2}$. □

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*

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

Proof. Now

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

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 is not congruent to 0 modulo 5 so not all of $i_1, 2i_2, \cdots, mi_m$ are congruent to 0 modulo 5. Suppose that ji_j is not congruent to 0 modulo 5. Then, in particular, i_j is not congruent to 0 modulo 5. But $0 \leq i_j \leq 5$ so $i_j \neq 0$. Thus none of $i_0, \ldots, i_m$ is equal to 5 since their sum is 5. Then

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

The result follows since $a_0^{i_0} \cdots a_m^{i_m}$ is an integer. □

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

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

Then

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

From the Euler Pentagonal Number Theorem and Theorem 2.1 we have

$$\begin{aligned}F(q) &= q \sum_{m=-\infty}^{\infty} (-1)^m q^{m(3m-1)/2} \sum_{k \geq 0} (-1)^k (2k+1) q^{\binom{k+1}{2}} \\ &= \sum_{m=-\infty, k \geq 0}^{\infty} (-1)^{m+k} (2k+1) q^{1 + m(3m-1)/2 + \binom{k+1}{2}}.\end{aligned}$$

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

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

so

$$p(5j-1) = \sum_{n \geq 0} \left([q^n] F(q)\right) \left(\left[q^{5j-n}\right] \prod_{k \geq 1} \left(1 - q^k\right)^{-5}\right). \tag{3}$$

There are two cases.

Case 1: *Assume that* $n \equiv 0$. Then $[q^n] F(q)$ is non-zero if $1 + m(3m-1)/2 + \binom{k+1}{2} \equiv n$. 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

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

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

$$\binom{k+1}{2} \equiv 3B^2 - 2B \text{ if } k \equiv B.$$

By direct computation,

$$\left(-A^2 + 2A + 1 \bmod 5\colon A = 0, \dots, 4\right) = (1, 2, 1, 3, 3)$$

and

$$\left(3B^2 - 2B \bmod 5\colon B = 0, \dots, 4\right) = (0, 1, 3, 1, 0).$$

Then $1 + m(3m-1)/2 + \binom{k+1}{2} \equiv 0$ 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 (3) is 0 from this case.

Case 2: *Assume that* n *is not congruent to* 0 *modulo* 5. Then neither is $5j - n$, so, from Lemma 2.2, $\left[q^{5j-n}\right] \prod_{k \geq 1} \left(1 - q^k\right)^{-5} \equiv 0$ since $\left(1 - q^k\right)^{-5}$ is a series with integer coefficients. It follows that the contribution to the right hand side of (3) is 0 in this case.

We conclude from (3) that $p(5j-1) \equiv 0$, establishing the result. □

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

$$G(q) = q^2 \prod_{i \geq 1} \left(1 - q^i\right)^6.$$

Then

$$G(q) = q^2 \prod_{i \geq 1} \left(1 - q^i\right)^3 \prod_{i \geq k} \left(1 - q^k\right)^3.$$

From Theorem 2.1 we have

$$G(q)=\sum_{j,k\geq 0}(-1)^{k+j}(2k+1)(2k+1)\,q^{2+\binom{j+1}{2}+\binom{k+1}{2}}.$$

Now note that $q^2\prod_{i\geq 1}\left(1-q^i\right)^{-1}=G(q)\prod_{k\geq 1}\left(1-q^k\right)^{-7}$. Then

$$\begin{aligned} p(7j-2) &= \left[q^{7j-2}\right]\left(1-q^i\right)^{-1}=\left[q^{7j}\right]G(q)\prod_{k\geq 1}\left(1-q^k\right)^{-7} \\ &= \sum_{n\geq 0}\left(\left[q^n\right]G(q)\right)\left(\left[q^{7j-n}\right]\prod_{k\geq 1}\left(1-q^k\right)^{-7}\right). \end{aligned}$$

so

$$p(7j-2)=\sum_{n\geq 0}\left(\left[q^n\right]G(q)\right)\left(\left[q^{7j-n}\right]\prod_{k\geq 1}\left(1-q^k\right)^{-7}\right) \tag{4}$$

There are two cases.

Case 1: *Assume that* $n\equiv 0$.We now proceed as before. It follows easily (the details are omitted) that

$$2+\binom{j+1}{2}+\binom{k+1}{2}\equiv(2A+1)^2+(2B+1)^2 \text{ if } j\equiv A \text{ and } k\equiv B.$$

But by direct computation

$$((2A+1) \bmod 5\colon A=0,\ldots,4)=(1,2,4,0,4,2,1)$$

so $2+\binom{j+1}{2}+\binom{k+1}{2}\equiv 0$ 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 $\left[q^n\right]G(q)\equiv 0$. Thus the contribution to the right hand side of (4) is 0 from this case.

Case 2: *Assume that n is not congruent to* 0 *modulo* 7. Then neither is $7j-n$, so, from the comment folowing Lemma 2.2, $\left[q^{7j-n}\right]\prod_{k\geq 1}\left(1-q^k\right)^{-7}\equiv 0$ since $\left(1-q^k\right)^{-7}$ is a series with integer coefficients. It follows that the contribution to the right hand side of (4) is 0 in this case.

We conclude from (4) that $p(7j-2)\equiv 0$, establishing the result. □