An identity for the number of partitions \( (\text{mod } \ell) \) of \( n \)

Quentin Gazda∗

Abstract

Let \( p(n) \) denotes the number of partitions of \( n \) and let \( \ell \geq 5 \) be a prime number. Let also \( \delta \) denotes \((\ell^2 - 1)/24\). For \( n < \ell^2 \), we prove a surprising identity \((\text{mod } \ell)\) between \( p(n - \delta) \) and the number of points in a certain subset of a lattice in \( \mathbb{R}^\ell \). The formula appears to be an easy consequence of the Macdonald identity for \( \mathfrak{sl}_\ell \), which we reprove and slightly extend using wronskians of vector-valued Jacobi forms of half-integral weight.

For a positive integer \( n \), let \( p(n) \) denotes the number of partitions of \( n \). In this short note, we prove a surprising identity for \( p(n) \) modulo a prime number \( \ell \geq 5 \) in terms of the number of points in a subset of a lattice in \( \mathbb{R}^\ell \). More precisely, we show

**Theorem 1.** Let \( \ell \geq 5 \) be a prime number and write \( \delta \) for \((\ell^2 - 1)/24\) (which is an integer). For all \( n < \ell^2 \), we have

\[
p(n - \delta) \equiv \left| \left\{ x \in \mathbb{Z}^\ell \mid \| x \|^2 = 2\ell n, \ |x| = 0, \ x \equiv (1, 2, ..., \ell) \ (\text{mod } \ell) \right\} \right| \ (\text{mod } \ell)
\]

where \( \| (x_1, ..., x_\ell) \|^2 = x_1^2 + ... + x_\ell^2 \) and \( |(x_1, ..., x_\ell)| = x_1 + ... + x_\ell \).

We did not find any comparable statement in the existing literature, which was rather unexpected, as the above theorem follows from a simple computation using the Macdonald identity for \( \mathfrak{sl}_\ell \). The story of partitions and Macdonald’s identities might date back to Winquist who used, in [Wi69], root systems of type \( B_2 \) to reprove Ramanujan congruence \((\text{mod } 11)\). The link between Macdonald’s identities and partitions goes as follow.

∗Current address: Univ Lyon, Université Jean Monnet Saint-Étienne, CNRS UMR 5208, Institut Camille Jordan, F-42023 Saint-Étienne, France
Let \( \eta \) denote the Dedekind \( \eta \)-function, given by the infinite product
\[
\eta(\tau) \overset{\text{def}}{=} q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n)
\]
where \( \mathcal{H} = \{ z \in \mathbb{C} | \text{im}(z) > 0 \} \) is the Poincaré upper-half plane, and \( q \) is the local parameter \( e^{2i\pi \tau} \) at infinity. There is a well-known relation between \( \eta \) and the generating series of the partition function, given by
\[
\prod_{n=1}^{\infty} (1 - q^n) = 1 + \sum_{n=1}^{\infty} p(n)q^n. \tag{1}
\]
On the other hand, let \( R \) be a reduced root system in a real vector space \( V \) canonically attached to a semi-simple Lie algebra \( g \) over \( \mathbb{C} \). Let \((\cdot, \cdot)\) be a scalar product on \( V \) invariant under the action of the Weyl group of \( R \). To settle notations, we let \( \|x\|^2 = (x, x) \) for \( x \in V \), we fix \( \Phi \) the highest root of \( R \) and set \( g = (\Phi, \rho) \) for \( \rho \) half the sum of the positive roots in \( R \) (positive being defined with respect to the early choice of a Weyl chamber). We let \( \Lambda \) be the lattice in \( V \) generated by the set \( \{ \frac{2g\alpha}{\|\alpha\|} | \alpha \in R \} \). In the celebrated paper \([Ma72]\), I. G. Macdonald proved a remarkable identity for the power of the Dedekind’s \( \eta \)-function:
\[
\eta(\tau)^{\dim g} = \sum_{l \in \Lambda} \prod_{\alpha > 0} \frac{(l + \rho, \alpha)}{(l, \alpha)} q^{\frac{\|l+\rho\|^2}{2g}} \quad (\tau \in \mathcal{H}). \tag{2}
\]
For \( n \) an odd positive integer and \( g = sl_n \), we draw from \([Ma72, \text{App. 1(6)(a)}]\) that equation (2) boils down to
\[
\eta(\tau)^{n^2 - 1} = \frac{1}{1!2! \cdots (n-1)!} \sum_{(x_1, \ldots, x_n) \in \mathbb{Z}^n} \prod_{i<j} (x_i - x_j) q^{\frac{1}{2}\left(x_1^2 + \cdots + x_n^2\right)} \tag{3}
\]
For \( n = 5 \), (3) is known as Dyson’s identity and is equivalent to a formula for Ramanujan function \( \tau \) (presented in \([Dy72]\)). Let \( \theta \) be the usual
\[
\theta(\tau, z) \overset{\text{def}}{=} \sum_{r \in \mathbb{Z}} q^{\frac{r^2}{2}} \zeta^r \quad (\zeta = e^{2i\pi z}, \ z \in \mathbb{C}).
\]
Using Wronskian of families of such functions, we are able to extend (3) to:
\[\textbf{Theorem 2.} \quad \text{Let } n \text{ be an odd positive integer. For all } \tau \in \mathcal{H}, \ z \in \mathbb{C}, \text{ we have}
\]
\[
\theta(\tau, z)\eta(\tau)^{n^2 - 1} = \frac{1}{1!2! \cdots (n-1)!} \sum_{(x_1, \ldots, x_n) \in \mathbb{Z}^n} \prod_{i<j} (x_i - x_j) q^{\frac{x_1^2 + \cdots + x_n^2}{2n}} \zeta^{\left(x_1 + \cdots + x_n\right)}
\]
where the sum is over \( n \)-tuples \( (x_1, \ldots, x_n) \) in \( \mathbb{Z}^n \) such that \( x_i \equiv i \pmod{n} \) for all \( i \).
An identity for the number of partitions (mod $\ell$) of $n$

Quentin Gazda

Since Theorem 1 follows from a particular case of Theorem 2, this note is mainly self-contained. Our methods are rather elementary and only use classical results for modular forms. In particular, our proof of Theorem 2 avoids the use of root systems of Lie algebras. The present paper is divided in two sections, each of them being the proof of the announced Theorem.

1 Proof of Theorem 1

Due to (1), we convenient that $p(0) = 1$ and $p(n) = 0$ for $n < 0$. For $\ell \geq 5$ we reduce the formula (3) for $n = \ell$ modulo $\ell$. For $(x_1, \ldots, x_\ell) \in \mathbb{Z}^\ell$ as in the summation indices of (3), Wilson’s theorem yields

$$\prod_{i<j}(x_i - x_j) \equiv \prod_{i<j}(i - j) \equiv 1!2! \cdots (\ell - 1)! \equiv 1 \pmod{\ell}.$$ 

One obtains:

$$q^\delta \prod_{n=1}^{\infty} \left(1 - q^n\right) \equiv \prod_{n=1}^{\infty} \left(1 - q^{\ell^2 n}\right) \sum_{(x_1, \ldots, x_\ell) \in \mathbb{Z}^\ell \atop x_i \equiv i \pmod{\ell}} q^\frac{1}{2}(x_1^2 + \cdots + x_\ell^2) \pmod{\ell}. $$

Writing down the Cauchy product on the right-hand side implies the following recursion formula for $p(n) \pmod{\ell}$, from which Theorem 1 is deduced.

**Proposition 1.** Let $\ell \geq 5$ be a prime number, and, for all integer $m$, let $c_\ell(m)$ denote the number of elements in the set

$$\{x \in \mathbb{Z}^\ell \mid \|x\|^2 = 2\ell m, \ |x| = 0, \ x \equiv (1, 2, \ldots, \ell) \pmod{\ell}\}. $$

Then, for all integer $n$,

$$p(n - \delta) \equiv \sum_{r=0}^{[n/\ell^2]} p(r)c_\ell(n - r\ell^2) \pmod{\ell}. $$

2 Proof of Theorem 2

We now turn to the proof of Theorem 2, which in particular will reprove Macdonald’s identity for $\mathfrak{sl}_n$ for odd $n$. Using similar methods, it seems possible to extend the former for $n$ even.

Let $\Gamma$ denote the following congruence subgroup of $\text{SL}_2(\mathbb{Z})$ of index 3:

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \pmod{2} \right\}. $$
An identity for the number of partitions (mod $\ell$) of $n$  
Quentin Gazda

It is generated by the two elements $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$.

As we will use them extensively, we introduce the classical slash operators for modular and Jacobi forms. For all integer $k$, we define the set $G_{k/2}(\Gamma)$ consisting in pairs $[\sigma, \varphi]$ where $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and where $\varphi : \mathcal{H} \to \mathbb{C}$ is a holomorphic function such that there exists a root of unity $t$ for which $\varphi(\tau)^2 = t^k(c\tau + d)^k$ (for all $\tau \in \mathcal{H}$). The function $\varphi$ will be referred as the automorphy factor (of weight $k/2$) of the pair. As usual, $j$ will be the automorphy factor $(\sigma, \tau) \mapsto c\tau + d$. For legibility, the dependence in $\sigma$ in the automorphy factor shall not appear. The set $G_{k/2}(\Gamma)$ is again a group according to the operation $[\sigma_1, \varphi_1][\sigma_2, \varphi_2] = [\sigma_1\sigma_2, \tau \mapsto \varphi_1(\sigma_2\tau)\varphi_2(\tau)]$. Note that for $\sigma \in \Gamma$, if $[\sigma, \varphi_1] \in G_{k_1/2}(\Gamma)$ and $[\sigma, \varphi_2] \in G_{k_2/2}(\Gamma)$, then $[\sigma, \varphi_1\varphi_2] \in G_{k_1+k_2/2}(\Gamma)$. For a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ and $[\sigma, \varphi] = [(a \ b \ c \ d), \varphi] \in G_{k/2}(\Gamma)$, let $(f | [\sigma, \varphi])$ be the holomorphic function given for all $\tau \in \mathcal{H}$ by

$$(f | [\sigma, \varphi])(\tau) \overset{\text{def}}{=} \varphi(\tau)^{-1} f \left( \frac{a\tau + b}{c\tau + d} \right).$$

Let $m$ be a rational number. For a function $\phi : \mathcal{H} \times \mathbb{C} \to \mathbb{C}$, holomorphic in its two variables, we also let

$$(\phi | [\sigma, \varphi])(\tau, z) \overset{\text{def}}{=} \varphi(\tau)^{-1} \exp \left( -\frac{2i\pi mcz^2}{c\tau + d} \right) \phi \left( \frac{a\tau + b}{c\tau + d} , \frac{z}{c\tau + d} \right).$$

We extend coordinate-wise the slash operators on vectors of functions. Note that the slash operator (4) was introduce to define Jacobi forms by Eichler and Zagier in [EZ85].

As for the classical slash operator, (4) is not stable by derivative in the variable $z$. There is, however, a relation to the Wronskian of a vector of functions. For $\Phi : \mathcal{H} \times \mathbb{C} \to \mathbb{C}^n$, we define

$$\text{Wron}_z \Phi \overset{\text{def}}{=} \det(\Phi, \partial_z \Phi, ..., \partial_z^{n-1} \Phi).$$

From Leibniz’ derivation rule, we have that $\partial_z^r(\phi | [\sigma, \varphi]) = (\partial_z^r \phi) | [\sigma, j^r\varphi] +$ a linear combination of $(\partial_z^r \phi) | [\sigma, j^i\varphi]$ ($i < r$) with complex coefficients independent of $\phi$. By multilinearity of $\det$, it appears that

$$\text{Wron}_z(\Phi | [\sigma, \varphi]) = (\text{Wron}_z \Phi) |_{mn} \left[ \sigma, j^{\frac{n(n-1)}{2}} \varphi^n \right].$$

If $[\sigma, \varphi]$ is in $G_{k/2}(\Gamma)$, $\left[ \sigma, j^{\frac{n(n-1)}{2}} \varphi^n \right]$ belongs to $G_{K/2}(\Gamma)$ where $K = n(n+k-1)$.

Let $n$ be an odd positive integer, and consider

$$\theta_{n,i}(\tau, z) \overset{\text{def}}{=} \sum_{x \equiv i \pmod{n}} q^{x^2 \zeta^x} \left( \zeta = e^{2i\pi z}, \ z \in \mathbb{C}, \ \tau \in \mathcal{H} \right).$$

Let $\theta_n$ be the transpose of $(\theta_{n,1}, ..., \theta_{n,n})$. The following Lemma is deduced from Poisson’s formula:
Lemma 1. There exists a unitary representation $u_n : \Gamma \rightarrow \text{GL}_n(\mathbb{C})$ such that, for all $\sigma \in \Gamma$, there exists $\varphi : \mathcal{H} \rightarrow \mathbb{C}$ for which $[\sigma, \varphi] \in G_{12}(\Gamma)$ and

$$ (\theta_n|_\varphi [\sigma, \varphi]) = u_n(\sigma)\theta_n. $$

As Lemma 1 is classical, we leave it without proof. The representation $u_n$ and the automorphy factor $\varphi$ can be made explicit, but for our purpose we simply need to know that $u_n$ is unitary. Note that the function $\theta$ of the introduction is here denoted $\theta_{1,0}$. By Lemma 1, $\theta$ is a weak $\mathbb{C}$-valued Jacobi form of weight and index $1/2$, level $\Gamma$ and type a certain character $u:=u_1$.

By (5) and for $[\sigma, \varphi]$ as in Lemma 1, we find that

$$ (\text{Wronz}_\varphi \theta_n)|_{\mathbb{Z}^n} \left[ \sigma, \frac{\pi(n-1)}{2} \varphi^n \right] = (\det u_n(\sigma)) (\text{Wronz}_\varphi \theta_n). $$

Vandermonde’s identity enables us to compute its Fourier expansion:

Lemma 2. For all $\tau \in \mathcal{H}$ and $z \in \mathbb{C}$, we have

$$ (\text{Wronz}_\varphi \theta_n)(\tau, z) = \sum_{(x_1, ..., x_n) \in \mathbb{Z}^n} \prod_{i<j} (x_i - x_j) q^{\frac{1}{2n}(x_i^2 + ... + x_n^2)} \zeta^{x_1 + ... + x_n}. $$

Proof. It is enough to prove the formula formally. We have

$$ \text{Wronz}_\varphi \theta_n = \det(\theta_n, \partial_x \theta_n, ..., \partial_x^{n-1} \theta_n) $$

$$ = \sum_{x_1, x_2, ..., \equiv 1, 2, ..., \text{mod } n} \det(1, (x_i)_i, ..., (x_i^{n-1})_i) q^{\frac{1}{2n}(x_i^2 + ... + x_n^2)} \zeta^{x_1 + ... + x_n}. $$

By Vandermonde’s identity, $\det(1, (x_i)_i, ..., (x_i^{n-1})_i) = \prod_{i<j} (x_i - x_j)$. 

This Lemma implies that $(\text{Wronz}_\varphi \theta_n)(\tau, z/n)$ is, up to a multiplicative factor, the member on the right-hand side in Theorem 2. The function appearing in (3) is rather related to $h_r$ that we now define. For $r \in \mathbb{Z}$, $\tau \in \mathcal{H}$, let

$$ h_r(\tau) = \sum_{(x_1, ..., x_n) \in \mathbb{Z}^n} \prod_{i<j} (x_i - x_j) q^{\frac{1}{2n}(x_i^2 + ... + x_n^2)} \zeta^{x_1 + ... + x_n}. $$

Note that, for all $\tau \in \mathcal{H}$ and $z \in \mathbb{C}$,

$$ (\text{Wronz}_\varphi \theta_n)(\tau, z) = \sum_{r \in \mathbb{Z}} h_r(\tau) q^{\frac{r^2}{2n}} \zeta^r. $$

On one hand, note that for $(x_1, ..., x_n)$ as in the summation indices of (7), the sum $x_1 + ... + x_n$ is always a multiple of $n$, as $n$ is odd. In particular, $h_r = 0$
An identity for the number of partitions (mod \( \ell \)) of \( n \)

Quentin Gazda

if \( r \) is not a multiple of \( n \).

On the other hand, we note that \( h_r \) depends only on its class (mod \( n^2 \)) by the change of indices \((x_1, ..., x_n) \mapsto (x_1 + n, ..., x_n + n)\). As \( n \) is odd, the change of indices \((x_2, ..., x_n, x_1) \mapsto (x_1 + 1, ..., x_{n-1} + 1, x_n + 1)\) implies \( h_r = h_{r+n} \).

Consequently, (8) becomes

\[
(Wronz_\theta n)(\tau, z) = h_0(\tau) \left( \sum_{r \in \mathbb{Z}} q^{r^2} \zeta^{rn} \right) = h_0(\tau) \theta(\tau, nz).
\]

By (6) and Lemma 1, we find that \( h_0 \) satisfies a modular invariance property:

\[
(Wronz_\theta n)(\tau, z) = (\det u_n(\sigma))^{-1} (Wronz_\theta n)|_{\sigma = \frac{n(n-1)}{2} \phi} (\tau, z) = (\det u_n(\sigma))^{-1} (h_0)|_{\sigma = \frac{n(n-1)}{2} \phi} \left[ \sigma, j^{\frac{n(n-1)}{2}} \phi^{n-1} \right](\tau)(\theta|_{1/2}[\sigma, \phi])(\tau, nz) = \frac{u(\sigma)}{\det u_n(\sigma)} (h_0)|_{\sigma = \frac{n(n-1)}{2} \phi} \left[ \sigma, j^{\frac{n(n-1)}{2}} \phi^{n-1} \right](\tau) \theta(\tau, nz),
\]

from which one deduce

\[
h_0|_{\sigma = \frac{n(n-1)}{2} \phi^{n-1}} = \frac{u(\sigma)}{\det u_n(\sigma)} h_0.
\]

In particular, \( h_0 \) behaves like a modular form of weight \( (n^2 - 1)/2 \) for \( \Gamma \) with some character \( \sigma \mapsto (\det u_n(\sigma))u(\sigma)^{-1} \) of norm 1. From the Fourier expansion (7) of \( h_0 \), the latter still holds if we replace \( \Gamma \) by \( SL_2(\mathbb{Z}) \) as \( h_0 \) is invariant by \( \tau \mapsto \tau + 1 \) up to the multiplication by a root of unity. Besides, its order of vanishing at the cusp infinity of \( SL_2(\mathbb{Z}) \) is at least

\[
\frac{1}{2n} \left( 1^2 + ... + \left( \frac{n-1}{2} \right)^2 + \left( \frac{n+1}{2} \right)^2 + ... + (-1)^2 \right) = \frac{n^2 - 1}{24}.
\]

Consequently, \( h_0/\eta^{n^2-1} \) is invariant of weight 0 for \( SL_2(\mathbb{Z}) \) (for some character of norm 1) and bounded on \( \mathcal{H} \). Therefore, it is a constant function on \( \mathcal{H} \). Identifying the constant to be \( 1!2! \cdots (m - 1)! \) as the first nonzero Fourier coefficient of \( h_0 \) finishes the proof of Theorem 2.

References

[Dy72] F. J. Dyson Missed opportunities, Bull. Amer. Math. Soc. 78 (1972) p. 191–201.

[EZ85] M. Eichler, D. Zagier The Theory of Jacobi Forms, Progress in Mathematics 55 (1985).
An identity for the number of partitions (mod $\ell$) of $n$

Quentin Gazda

[Ma72] I. G. Macdonald *Affine root systems and Dedekind’s $\eta$-function*, Invent. Math. 15 (1972) p. 91–143.

[Wi69] L. Winquist *Elementary proof of $p(11m + 6) \equiv 0$ (mod 11)*, J. Comb. Theory 6 (1969) p. 56–59.