

# The arithmetic of supersymmetric vacua

---

**Antoine Bourget and Jan Troost**

*Laboratoire de Physique Théorique de l'École Normale Supérieure,  
CNRS, PSL Research University, Sorbonne Universités,  
75005 Paris, France*

*E-mail:* [bourget@lpt.ens.fr](mailto:bourget@lpt.ens.fr), [troost@lpt.ens.fr](mailto:troost@lpt.ens.fr)

**ABSTRACT:** We provide explicit formulas for the number of vacua of four-dimensional pure  $\mathcal{N} = 1$  super Yang-Mills theories on a circle, with any simple gauge algebra and any choice of center and spectrum of line operators. The formula for the  $(\mathrm{SU}(N)/\mathbb{Z}_m)_n$  theory is a key ingredient in the semi-classical calculation of the number of massive vacua of  $\mathcal{N} = 1^*$  gauge theories with gauge algebra  $\mathfrak{su}(n)$ , compactified on a circle. Using arithmetic, we express that number in an  $\mathrm{SL}(2, \mathbb{Z})$  duality invariant manner. We confirm our tally of massive vacua of the  $\mathcal{N} = 1^*$  theories by a count of inequivalent extrema of the exact superpotential.

**KEYWORDS:** Supersymmetric gauge theory, Duality in Gauge Field Theories, Wilson, 't Hooft and Polyakov loops

**ARXIV EPRINT:** [1606.01022](https://arxiv.org/abs/1606.01022)

---

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>The index of pure supersymmetric Yang-Mills theories on a circle</b>	<b>2</b>
<b>3</b>	<b>The index of <math>\mathcal{N} = 1^*</math> gauge theories on a circle</b>	<b>3</b>
3.1	The semi-classical calculation of the index	3
3.2	The arithmetic heart	6
3.3	Duality invariance	7
3.4	The exact superpotential approach	8
<b>4</b>	<b>Conclusions</b>	<b>12</b>
<b>A</b>	<b>Supersymmetric indices of pure <math>\mathcal{N} = 1</math> Yang-Mills theories</b>	<b>12</b>
<b>B</b>	<b>The details and the arithmetic</b>	<b>15</b>
B.1	The unbroken gauge group	15
B.2	A warm-up for $S$ -duality	16
B.3	A sum of greatest common divisors	17
B.4	Auxiliary lemmas	17

---

## 1 Introduction

The calculation of the number of vacua of pure  $\mathcal{N} = 1$  super Yang-Mills theories on  $\mathbb{R}^4$  is non-trivial, as witnessed by the seventeen years it took to spell out its subtleties [1–8]. The final result for a theory with simple gauge algebra  $\mathfrak{g}$  is that the theory has a number of massive vacua equal to the dual Coxeter number of the gauge algebra, as predicted by chiral symmetry breaking. Only recently it was made manifest that when we compactify the theory on a circle, further subtleties need to be taken into account to provide the tally of massive vacua [9]. In particular, the choice of the center of the simple gauge group as well as the spectrum of line operators in the theory influence the supersymmetric index of pure  $\mathcal{N} = 1$  super Yang-Mills theory on a circle [9]. The reasoning of how to calculate the number of vacua in all cases was laid out in [9, 10], and an explicit formula was given for almost all cases.<sup>1</sup>

In this paper, we firstly complete the list of explicit formulas for the supersymmetric index of the pure  $\mathcal{N} = 1$  theory on a circle. In the bulk of the paper, we calculate the number of vacua for the  $SU(N)/\mathbb{Z}_m$  gauge theory, with a spectrum of line operators further

---

<sup>1</sup>See [11] for further analysis of the dynamics in the non-supersymmetric setting.

specified by an integer  $n$  modulo  $m$  [9]. The index is a sum over greatest common divisors. All other cases that were left aside in [9] are rendered explicit in appendix A.

Secondly, we compute the number of vacua of  $\mathcal{N} = 4$  supersymmetric Yang-Mills theories with gauge algebra  $\mathfrak{su}(n)$ , deformed by three mass terms for the adjoint chiral multiplets to the  $\mathcal{N} = 1^*$  theory. We count the massive vacua upon circle compactification semi-classically, by classifying gauge group breaking patterns [12, 13], including discrete gauge group factors, and using the index for the pure supersymmetric Yang-Mills theory on  $\mathbb{R}^3 \times S^1$ . The final result is an intricate combination of elementary arithmetic functions.

Thirdly, we show that the semi-classical counting function can be rewritten, with some arithmetic effort, in terms of an  $SL(2, \mathbb{Z})$  invariant expression, thus proving the consistency of the semi-classical analysis with the duality invariance of the parent  $\mathcal{N} = 4$  theory. Finally, we confirm our census by an analysis of inequivalent extrema of the exact elliptic superpotential [13].

## 2 The index of pure supersymmetric Yang-Mills theories on a circle

Pure  $\mathcal{N} = 1$  theories in four dimensions with a simple gauge algebra  $\mathfrak{g}$  permit a choice of global gauge group and spectrum of line operators [9, 10]. Our goal in this section and appendix A is to complete the list of explicit formulas for the supersymmetric index of all  $\mathcal{N} = 1$  theories, following the path laid out in [9].

The first remaining case is the theory with (electric) gauge group  $G = SU(N)/\mathbb{Z}_m$ , and a spectrum of line operators with charges  $(m, 0)\mathbb{Z} + (n, \frac{N}{m})\mathbb{Z}$ , where both electric and magnetic entries are defined modulo  $N$ . The charges are representations of the electric times magnetic center groups  $\mathbb{Z}_N \times \mathbb{Z}_N$ , and classify the possible physical behaviours of loop operators.<sup>2</sup> The resulting theory is referred to as the  $(SU(N)/\mathbb{Z}_m)_n$  theory. The number  $m$  is a divisor of  $N$ , and fixes the global choice of gauge group (via a choice of center). The integer  $n$  is defined modulo  $m$  and captures a choice of complete set of line operators. This case will play into the rest of the paper, and we therefore treat it in the main text. All remaining cases are discussed in appendix A.

We calculate the number of vacua of the  $(SU(N)/\mathbb{Z}_m)_n$  theory upon compactification on a circle following the reasoning described in [9]. Firstly, we note that if we consider any pure  $\mathcal{N} = 1$ ,  $\mathfrak{su}(n)$  theory on  $\mathbb{R}^4$ , then it has  $N$  vacua. In the  $(SU(N)/\mathbb{Z}_m)_n$  theory, there is a global symmetry group  $\mathbb{Z}_{\frac{N}{m}}$  that exchanges vacua. We will label  $m$  inequivalent vacua by  $l = 1, \dots, m$ , in such a way that condensed particles in vacuum  $l$  have a dyonic tilt equal to  $-l$  at  $\theta$ -angle equal to zero.

Secondly, we consider the vacuum  $l$ . It is convenient to map the dyons into purely magnetic objects by shifting the  $\theta$ -angle by  $2\pi l$ . After this transformation, the electric charge of each line operator is shifted by  $l$  times its magnetic charge, as a consequence of the Witten effect. Thus, after this shift, we are left with a spectrum of line operator charges which is equal to

$$\left( qm + p \left( n + l \frac{N}{m} \right), p \frac{N}{m} \right) \tag{2.1}$$

---

<sup>2</sup>We refer to [9] for a pedagogical introduction of the relevant concepts.

with  $q, p$  arbitrary integers, and purely magnetic condensates. We conclude that for non-zero electric charge  $qm + p(n + l\frac{N}{m})$  modulo  $N$ , the line operator exhibits an area law, while if this quantity is zero (modulo  $N$ ), the line operator satisfies a perimeter law. A non-trivial purely magnetic line operator with a perimeter law indicates the existence of an unbroken magnetic gauge symmetry.

To identify the unbroken symmetry group, we determine the purely magnetic line operator with the smallest charge. This line operator generates the algebra of purely magnetic line operators. Its charge can be written as  $(0, p\frac{N}{m})$  where  $p$  is the smallest positive integer such that

$$\exists q \in \mathbb{Z} : qm + p \left( n + l\frac{N}{m} \right) = 0 \quad \text{modulo } N. \tag{2.2}$$

Since  $m|N$ , this implies that  $p(n + l\frac{N}{m}) = 0$  modulo  $m$ . Let's introduce  $r = \text{gcd}(m, n + l\frac{N}{m})$ . We can divide the equation by  $r$  and then infer that the solution for  $p$  is 0 modulo  $\frac{m}{r}$ . Thus, we finally have magnetic line operators with charges  $(0, \frac{N}{r})\mathbb{Z}$ . These 't Hooft line operators have perimeter law. This shows the existence of an unbroken magnetic gauge group  $\mathbb{Z}_r \subset \mathbb{Z}_m$  in the  $l$ -th vacuum. Thus, each vacuum  $l$ , upon compactification on a circle, obtains a multiplicity equal to  $r$ . We conclude that the supersymmetric index  $I$  counting massive vacua of the  $(\text{SU}(N)/\mathbb{Z}_m)_n$  pure  $\mathcal{N} = 1$  theory is equal to

$$I^{\mathcal{N}=1}(N, m, n) = \frac{N}{m} \sum_{l=1}^m \text{gcd} \left( m, n + \frac{lN}{m} \right). \tag{2.3}$$

Thus, we have accomplished our first task of providing an explicit formula for the supersymmetric index for all choices of  $(N, m, n)$ . We refer to appendix A for a table of results for all simple Lie algebras.

### 3 The index of $\mathcal{N} = 1^*$ gauge theories on a circle

In this section, we study  $\mathcal{N} = 4$  super Yang-Mills theories deformed by three supersymmetric mass terms for the three  $\mathcal{N} = 1$  chiral multiplets in the adjoint. We wish to compute the supersymmetric index for these  $\mathcal{N} = 1^*$  theories on the manifold  $\mathbb{R}^3 \times S^1$  and for an  $\mathfrak{su}(n)$  gauge algebra. The two main ingredients will be an analysis of the pattern of unbroken non-abelian gauge groups including discrete gauge group factors, and the supersymmetric index of pure  $\mathcal{N} = 1$  that we computed in section 2.

#### 3.1 The semi-classical calculation of the index

The number of massive vacua of the  $\mathcal{N} = 1^*$  theory on  $\mathbb{R}^4$  with gauge algebra  $\mathfrak{su}(N)$  is equal to  $\sigma_1(N)$ , the sum of the divisors of  $N$  [12]. We wish to generalize this counting function to the number of massive vacua for all  $\mathcal{N} = 1^*$  theories with  $\mathfrak{su}(N)$  algebra compactified on a circle. In this section, we count the vacua using semi-classical techniques.

We briefly review the analysis of the classical vacua of the theory [12–14]. The vacuum expectation values of the three adjoint scalar fields are in one-to-one correspondence with

the nilpotent orbits of  $\mathfrak{su}(N)$ , because they satisfy an  $\mathfrak{sl}(2)$  algebra due to the F-term equations of motions, and because the Jacobson-Morozov theorem provides a bijection between the  $\mathfrak{sl}(2)$  algebras embedded in the Lie algebra and the nilpotent orbits. The conjugacy classes of nilpotent orbits are moreover in bijection with integer partitions of  $N$ . Thus, we consider a partition

$$N = \underbrace{1 + \dots + 1}_{r_1} + \underbrace{2 + \dots + 2}_{r_2} + \dots = \sum_{i=1}^N r_i \times i, \tag{3.1}$$

where the integers  $r_i$  count representations of  $\mathfrak{sl}(2)$  of dimension  $i$ .

**The unbroken gauge group.** The centralizer of the corresponding  $\mathfrak{sl}(2)$ -triple (which are the vacuum expectation values of the adjoint scalar fields) in the simply connected complexified gauge group  $\mathrm{SL}(n, \mathbb{C})$  is (see e.g. [15]):

$$H_{\mathbb{C}} = S \left( \prod_{i=1}^N [\mathrm{GL}(r_i)]_{\Delta}^i \right). \tag{3.2}$$

The symbol  $\Delta$  is there to remind us that we diagonally embed  $\mathrm{GL}(r_i)$  inside  $i$  copies of the group. The symbol  $S$  indicates that the total determinant equals one.<sup>3</sup> If the complexified gauge group is  $G_{\mathbb{C}} = \mathrm{SL}(n, \mathbb{C})/\mathbb{Z}_m$ , with  $m$  a divisor of  $n$ , then the centralizer is obtained by dividing the group (3.2) by  $\mathbb{Z}_m$ .

We first observe that for a partition which contains two different integers, there will be an abelian gauge group factor. The partition will only give rise to massless vacua.<sup>4</sup> Thus, to obtain massive vacua, we consider  $d$  representations of dimension  $\frac{N}{d}$ , where  $d$  divides  $N$ . In this configuration for the adjoint scalars, the unbroken gauge group is

$$H_{\mathbb{C}} = S \left( (\mathrm{GL}(d))_{\Delta}^{\frac{N}{d}} \right) \cap G_{\mathbb{C}}. \tag{3.3}$$

In the low-energy limit, our initial  $\mathfrak{su}(N)$ ,  $\mathcal{N} = 1^*$  theory becomes a pure  $\mathcal{N} = 1$  theory with unbroken gauge group equal to the compact form of the group (3.3). We wish to rewrite the unbroken group (3.3) in a more recognizable form.

The non-abelian gauge algebra will be  $\mathfrak{sl}(d)$  where  $d|N$ . The covering group  $\mathrm{SL}(d)$  has a  $\mathbb{Z}_d$  center. We wish to mod out this center by  $\mathbb{Z}_m$ . To do this division, we work in the subgroup  $\mathbb{Z}_{\mathrm{lcm}(m,d)} \subset \mathbb{Z}_N$ . After division by  $\mathbb{Z}_m$ , we are left with a  $\mathbb{Z}_{\mathrm{lcm}(m,d)/m}$  center for the group generated by  $\mathfrak{sl}(d)$ . In other words, the center of the non-abelian gauge group will be  $\mathbb{Z}_{d/\mathrm{gcd}(m,d)}$ . Furthermore, the original center of the group was  $\mathbb{Z}_{N/m}$ . We therefore must have another discrete factor equal to  $\mathbb{Z}_{N\mathrm{gcd}(d,m)/(md)} = \mathbb{Z}_{N/\mathrm{lcm}(d,m)}$ . Since we can think of the center elements as matrices proportional to the identity, these groups will form a direct product. Thus, we find the centralizer:

$$H_{\mathbb{C}} = \mathbb{Z}_{N/\mathrm{lcm}(d,m)} \times \mathrm{SL}(d)/\mathbb{Z}_{\mathrm{gcd}(m,d)}. \tag{3.4}$$

<sup>3</sup>See [14] for details in the spirit of the present analysis.

<sup>4</sup>It is important to note that the unbroken gauge group does not allow for discrete Wilson lines on the circle that would break the abelian gauge group factors and leave a non-abelian unbroken gauge group after compactification. For other gauge algebras, this phenomenon does occur [16, 17].

In compact real form, the unbroken gauge group is

$$H = \mathbb{Z}_{N/\text{lcm}(d,m)} \times \text{SU}(d)/\mathbb{Z}_{\text{gcd}(m,d)}. \quad (3.5)$$

A more detailed version of the calculation of the unbroken gauge group is given in appendix B.1.

**The index.** We have determined how the numbers  $(N, m)$  characterizing the gauge group are inherited by an effective  $\mathcal{N} = 1$  theory that arises at low energy in the relevant adjoint scalar configurations labelled by a divisor  $d$  of  $N$ . We further observe that the number  $n$  determining the dyonic tilt of the spectrum of line operators is simply inherited by the effective pure  $\mathcal{N} = 1$  theory (albeit defined modulo  $\text{gcd}(m, d)$ ). Thus, we are ready to compute the index.

The overall discrete electric gauge group  $\mathbb{Z}_{N/\text{lcm}(d,m)}$  allows us to turn on electric Wilson lines that provide an extra multiplicity to the vacua of the pure  $(\text{SU}(d)/\mathbb{Z}_{\text{gcd}(m,d)})_n$  theories at low energy. Thus, we combine the form of the centralizer (3.5) and the index for the pure  $\mathcal{N} = 1$  theory (2.3) to compose the index for the  $\mathcal{N} = 1^*$   $(\text{SU}(N)/\mathbb{Z}_m)_n$  theory:

$$\begin{aligned} I^{\mathcal{N}=1^*}(N, m, n) &= \sum_{d|N} \frac{N}{\text{lcm}(m, d)} I^{\mathcal{N}=1}(d, \text{gcd}(m, d), n) \\ &= \sum_{d|N} \frac{N}{\text{lcm}(m, d)} \times \frac{d}{\text{gcd}(m, d)} \sum_{l=1}^{\text{gcd}(m,d)} \text{gcd} \left( \text{gcd}(m, d), n + \frac{ld}{\text{gcd}(m, d)} \right), \end{aligned} \quad (3.6)$$

and we finally find

$$I^{\mathcal{N}=1^*}(N, m, n) = \frac{N}{m} \sum_{d|N} \sum_{l=1}^{\text{gcd}(d,m)} \text{gcd} \left( \text{gcd}(d, m), n + \frac{ld}{\text{gcd}(d, m)} \right). \quad (3.7)$$

For pedagogical purposes, we list two special cases:

- For the  $\text{SU}(N)$  theory, we find the index

$$I^{\mathcal{N}=1^*}(N, 1, 0) = N \sum_{d|N} 1 = N\sigma_0(N). \quad (3.8)$$

- For the  $\text{SU}(N)/\mathbb{Z}_N$  theories, the number of massive vacua on the circle is

$$I^{\mathcal{N}=1^*}(N, N, n) = \sum_{d|N} \sum_{l=1}^d \text{gcd}(d, l). \quad (3.9)$$

In subsection 3.3, we will study the duality invariance of the general index formula (3.7), inherited from the parent  $\mathcal{N} = 4$  theory. We have just presented two special cases (3.8) and (3.9) of the counting function that are predicted to be the same by  $S$ -duality. The reader can choose to take a break in appendix B.2 where we prove the equality of these two indices. Inspired by these preliminaries, we unpack in the next subsection the surprises that the boxed arithmetic index (3.7) has in store.

### 3.2 The arithmetic heart

In this subsection, we regroup the contributions to the index (3.7) by the divisors  $d$  of  $N$ . In order to perform the regrouping, we need various arithmetic identities that we will first prove using elementary number theory.

Firstly, we recall three classical identities involving the Möbius function  $\mu$  and the Euler totient function  $\varphi$ :

$$\sum_{d|n} \mu(d) = \delta[n = 1], \quad \sum_{d|n} \varphi(d) = n, \quad \sum_{d|n} d\mu\left(\frac{n}{d}\right) = \varphi(n). \quad (3.10)$$

The function  $\delta[n = 1]$  is the unit function, which is unity when  $n = 1$  and zero on any integer larger than one. It is the identity element of Dirichlet convolution.<sup>5</sup> The first identity can be rephrased as the fact that the Möbius function in Dirichlet convolution with the constant function equal to one is the unit function,  $\mu * 1 = \delta$ . The second equality, proven in formula (B.9), expresses the fact that the Euler totient function convoluted with the constant function equals the identity function,  $\varphi * 1 = \text{id}$ . The third identity, which can be written  $\text{id} * \mu = \varphi$ , is a consequence of the other two.<sup>6</sup>

Secondly, we will need the more advanced formula [21]

$$\sum_{s=1}^n \gcd(n, as + b) = n \sum_{d|n} \frac{\varphi(d)}{d} \gcd(a, d) \delta[\gcd(a, d)|b], \quad (3.11)$$

whose proof is recalled in appendix B.3. The  $\delta$ -function again evaluates to one if the condition inside the bracket is satisfied, and to zero otherwise.

Thus, we are armed with the necessary tools to regroup the index for the  $\mathcal{N} = 1^*$  theory. We start from formula (3.7), and recount:

$$\begin{aligned} I^{\mathcal{N}=1^*}(N, m, n) &= \frac{N}{m} \sum_{d|N} \sum_{k=1}^{\gcd(d,m)} \gcd\left(\gcd(d, m), n + \frac{kd}{\gcd(d, m)}\right) \\ &= \frac{N}{m} \sum_{d|N} \sum_{e|\gcd(d,m)} \frac{\varphi(e)}{e} \gcd(d, m) \gcd\left(\frac{d}{\gcd(d, m)}, e\right) \delta\left[\gcd\left(\frac{d}{\gcd(d, m)}, e\right) | n\right] \\ &= \frac{N}{m} \sum_{d|N} \sum_{e|\gcd(d,m)} \frac{\varphi(e)}{e} \gcd(d, me) \delta\left[\gcd\left(\frac{d}{\gcd(d, m)}, e\right) | n\right] \\ &= \frac{N}{m} \sum_{e|m} \sum_{d|N} \frac{\varphi(e)}{e} \gcd(d, me) \delta\left[\gcd\left(\frac{d}{\gcd(d, m)}, e\right) | n\right] \\ &= \frac{N}{m} \sum_{e|m} \sum_{d|\frac{N}{e}} \varphi(e) \gcd(d, m) \delta\left[\gcd\left(\frac{de}{\gcd(de, m)}, e\right) | n\right]. \end{aligned} \quad (3.12)$$

<sup>5</sup>The Dirichlet convolution of two functions  $f, g$  defined on the positive integers is given by the formula  $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$ .

<sup>6</sup>Many elementary textbooks in arithmetic contain these facts. The last equation for instance dates back to Gauss.

We now simplify the condition in the  $\delta$ -function. For any divisor  $e$  of  $m$  and any divisor  $d$  of  $\frac{N}{e}$ , we have

$$\begin{aligned}
 \gcd\left(\frac{de}{\gcd(de, m)}, e\right) | n &\Leftrightarrow e \times \gcd(d, m) | n \times \gcd(de, m) \\
 &\Leftrightarrow \frac{\gcd(d, m)}{\gcd(d, \frac{m}{e})} | n \\
 &\Leftrightarrow \gcd(d, m) | dn \quad \text{and} \quad \gcd(d, m) | \frac{mn}{e} \\
 &\Leftrightarrow e | \frac{mn}{\gcd(d, m)}. \tag{3.13}
 \end{aligned}$$

We go back to the computation, and use the third identity in (3.10):

$$\begin{aligned}
 I^{\mathcal{N}=1^*}(N, m, n) &= \frac{N}{m} \sum_{e|m} \sum_{d|\frac{N}{e}} \varphi(e) \gcd(d, m) \delta\left[e | \frac{mn}{\gcd(d, m)}\right] \\
 &= \frac{N}{m} \sum_{d|N} \gcd(d, m) \sum_{e|\gcd(m, \frac{N}{d}, \frac{mn}{\gcd(d, m)})} \varphi(e) \\
 &= \frac{N}{m} \sum_{d|N} \gcd(d, m) \gcd\left(m, \frac{N}{d}, \frac{mn}{\gcd(d, m)}\right), \tag{3.14}
 \end{aligned}$$

and the last line simplifies to our final formula:

$$I^{\mathcal{N}=1^*}(N, m, n) = N \sum_{d|N} \gcd\left(d, m, \frac{N}{d}, \frac{N}{m}, n\right). \tag{3.15}$$

The original index formula (3.7) provides information on how each semi-classical pure  $\mathcal{N} = 1$  vacuum obtains a degeneracy upon compactification. The formula (3.15) regroups all contributions by the gauge group symmetry breaking pattern only.

### 3.3 Duality invariance

With the formula (3.15) in hand, we check the duality invariance of the index of  $\mathcal{N} = 1^*$  theory compactified on a circle. The parent  $\mathcal{N} = 4$  supersymmetric Yang-Mills theory with  $\mathfrak{su}(N)$  gauge algebra takes on  $\sigma_1(N) = \sum_{d|N} d$  different guises, depending on the choice of center and the dyonic tilt in the spectrum of line operators. The duality group that leaves invariant a given theory is  $\Gamma_0(N)$ , while the  $\text{SL}(2, \mathbb{Z})$  action on the coupling maps a theory to an equivalent one, with another choice of global gauge group and spectrum of line operators [9]. The  $\mathcal{N} = 1^*$  theory inherits these duality properties from its  $\mathcal{N} = 4$  parent. (See e.g. [18] for a detailed discussion.)

We recall the duality transformation rules from [9]. The  $T$ -duality maps the following theories into each other:

$$T : \left(\frac{\text{SU}(N)}{\mathbb{Z}_m}\right)_n \longrightarrow \left(\frac{\text{SU}(N)}{\mathbb{Z}_m}\right)_{n+\frac{N}{m}}. \tag{3.16}$$



In formula (3.7), the shift  $n \rightarrow n + \frac{N}{m}$  can be offset by a shift  $l \rightarrow l - \frac{N}{\text{lcm}(d,m)}$ . It is natural to find  $T$ -duality realized in the semi-classical counting because  $T$ -duality reshuffles the sum over pure  $\mathcal{N} = 1$  vacua in a straightforward manner. This proves that the index (3.7) is  $T$ -invariant. In the guise (3.15), with vacua grouped by divisors of  $N$  only,  $T$ -duality is also manifest.

On the other hand, only in the grouped formula (3.15) is  $S$ -duality manifest. Let us first note that when  $n = 0$ ,  $S$ -duality boils down to the exchange  $m \leftrightarrow \frac{N}{m}$ , which is a symmetry of (3.15). More generally,  $S$ -duality can be seen as the symmetry exchanging  $m$  and  $\text{gcd}(m, n)$ . Concretely, if two theories

$$S : \left( \frac{\text{SU}(N)}{\mathbb{Z}_m} \right)_n \longleftrightarrow \left( \frac{\text{SU}(N)}{\mathbb{Z}_{m'}} \right)_{n'} \tag{3.17}$$

are  $S$ -dual, then we have

$$m' = \frac{N}{\text{gcd}(m, n)}, \quad \text{gcd}(m', n') = \frac{N}{m}. \tag{3.18}$$

Armed with this knowledge, we can write

$$I^{\mathcal{N}=1^*}(N, m, n) = N \sum_{d|N} \text{gcd} \left( d, \frac{N}{d}, \frac{N}{m}, \text{gcd}(m, n) \right), \tag{3.19}$$

which renders  $S$ -duality evident.

### 3.4 The exact superpotential approach

In this subsection, we reproduce the index formula from a description of the full quantum dynamics of the theory compactified on a circle. A third guise of the supersymmetric index will be found. Our tool of choice is the effective elliptic superpotential  $\mathcal{W}$  derived in [13], which is a function of the Wilson line and dual photon variables in the Cartan subalgebra, that are the natural variables on the Coulomb branch upon compactification. As discussed in detail in [16, 17], the resulting elliptic Calogero-Moser integrable potential has a periodicity equal to the fundamental weight lattice both in the electric (Wilson line) direction (parametrized by real multiples of the complex number  $\tau$  say), as well as in the magnetic (dual photon) direction (parametrized by real numbers). In the gauge theory, however, we have a larger set of gauge inequivalent variables, and we must consider a  $N$ -fold cover of the fundamental torus of the integrable system, corresponding to identifications of the Cartan variables under shifts by the root lattice. Let's normalize the integrable system variables such that the fundamental torus has periodicities 1 and  $\tau$  in the dual photon and Wilson line directions respectively. We moreover denote multiples of the fundamental torus periods by the pairs  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ . From the spectrum of line operators in the theory  $(\text{SU}(N)/\mathbb{Z}_m)_n$ , it then follows that gauge transformations identify each individual Cartan variable under shifts in  $(m, 0)\mathbb{Z} + (-n, \frac{N}{m})\mathbb{Z}$ .<sup>7</sup>

<sup>7</sup>To prove this, it is sufficient to consider all gauge invariant Wilson-'t Hooft line operators, and perform constant shifts on the vacuum expectation values of the electric and magnetic gauge fields.

Theory	Partition $2 = 1 + 1$	Partition $2 = 2$	Total
SU(2)	SU(2) $\rightarrow$ 1 + 1 vacua	$\mathbb{Z}_2 \rightarrow$ 2 vacua	4
SO(3) <sub>+</sub>	SO(3) <sub>+</sub> $\rightarrow$ 2 + 1 vacua	1 $\rightarrow$ 1 vacuum	4
SO(3) <sub>-</sub>	SO(3) <sub>-</sub> $\rightarrow$ 1 + 2 vacua	1 $\rightarrow$ 1 vacuum	4

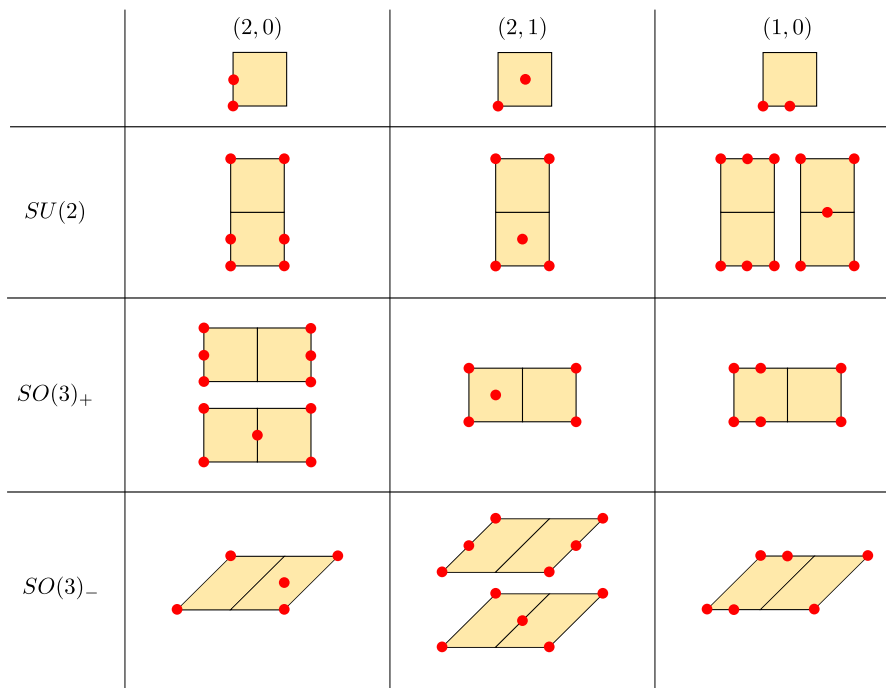
**Table 1.** An example of  $\mathcal{N} = 1^* \mathfrak{su}(2)$  vacua on the circle.

In a second stage, we recall that all the massive vacua, when projected onto the fundamental torus are described by index  $N$  lattice extensions of the fundamental torus [12, 13]. These lattices are coded in an integer  $d$  and a tilt  $t$ , and give rise to  $N$  points on the fundamental torus, which are all distinct multiples of  $(d/N, 0)$  and  $(t/N, 1/d)$ . Because we are dealing with the  $\mathfrak{su}(n)$  gauge algebra, the  $N$  points of the integrable system are only determined up to an overall arbitrary shift.

We must count the solutions of the gauge theory exact superpotential (with the gauge theory notion of inequivalence), which project onto these lattices in the fundamental torus. We illustrate the above notions concretely in the example of the gauge algebra  $\mathfrak{su}(2)$ , before counting inequivalent solutions in the general case.

**An example: the  $\mathfrak{su}(2)$  gauge algebra.** For the SU(2) gauge group, we have one Wilson line proportional to  $\tau$ , and periodic with period  $2\tau$ , arising from identifications of the Wilson line up to shifts in the root lattice. The dual photon has a period which is equal to the weight lattice. The complexified coordinate  $Z$  in the Cartan subalgebra thus lives in a double cover of the torus, with periods  $(1, 0)$  and  $(0, 2\tau)$ . We can count the vacua semi-classically following the analysis in subsection 3.1. We have two nilpotent orbits, corresponding to the partitions  $1 + 1$  and  $2$ . The first choice gives rise to two confining vacua of pure  $\mathcal{N} = 1$  SU(2), while the second yields two Higgsed vacua, with differing discrete Wilson lines, due to an unbroken  $\mathbb{Z}_2$  discrete gauge group. The non-zero discrete Wilson line shifts the coordinate  $Z$  by  $\tau$ . The confining vacuum has Wilson lines which are fixed by the exact effective superpotential. If one attempts to add a Wilson line to a confining vacuum, it is again gauge equivalent to a confining vacuum. This describes the situation for the SU(2) gauge group. The vacua are illustrated in the second line of figure 1 and table 1.

For the SO(3)<sub>+</sub> theory, we have periodicities  $(2, 0)$  and  $(0, \tau)$  and  $3 + 1$  semi-classical vacua, and similarly for the SO(3)<sub>-</sub> case, where the periodicities are  $(2, 0)$  and  $(0, \tau + 1)$ . The magnetic  $\mathbb{Z}_2$  gauge group arising in the pure  $\mathcal{N} = 1$  SO(3)<sub>±</sub> theories permits a magnetic Wilson line leading to a third non-gauge-equivalent vacuum, while the Higgs vacuum in these theories is unique. For these two theories as well, we draw the relevant double covers, and exhibit the four inequivalent vacua on each of these tori in figure 1. We also summarize the data in table 1. These three theories are mapped into each other under  $SL(2, \mathbb{Z})/\Gamma_0(2)$ , and in this way we verify the duality invariance of the index, equal to four in all theories.



**Figure 1.** We draw the double cover of the torus on which the complexified gauge theory Wilson line lives. The double cover depends on the theory. In the resulting torus, we draw the inequivalent extrema of the effective superpotential. The first two columns correspond to the confining theory, partition  $1 + 1$ , and the third column corresponds to the Higgs vacua, partition  $2$ . The top line provides the projection of the extrema onto the fundamental torus.

**The analysis for  $\mathfrak{su}(n)$ .** Let's finally count the number of inequivalent massive extrema in the case of the  $\mathfrak{su}(n)$  theories characterized by the integers  $(N, m, n)$ . Consider a configuration  $(d, t)$  of the integrable system (i.e. projected on the fundamental torus), and lift it to the gauge theory torus parametrized by  $(N, m, n)$ . We want to enumerate the inequivalent configurations, under the following equivalence relation. For any  $u \in \mathbb{Z}^2$ , the two configurations  $(X_1, \dots, X_N)$  and  $(X_1, \dots, X_i + u, \dots, X_j - u, \dots, X_N)$  are equivalent due to the identification of gauge theory variables under root lattice shifts. Furthermore, the ordering of the elements in the  $N$ -plet  $(X_1, \dots, X_N)$  is irrelevant because of the action of the Weyl group. It is clear that any configuration is equivalent to a reduced one where  $X_i \in [0, 1]^2$  for  $1 \leq i \leq N - 1$ . Moreover, given a configuration characterized by the numbers  $(d, t)$ , one can show that

$$(X_1, \dots, X_{N-1}, X_N) \sim (X_1, \dots, X_{N-1}, X_N + u_1) \sim (X_1, \dots, X_{N-1}, X_N + u_2) \quad (3.20)$$

where  $u_1 = (d, 0)$  and  $u_2 = (t, \frac{N}{d})$ . Because of the invariance of all line operators under gauge transformations, we also have

$$(X_1, \dots, X_{N-1}, X_N) \sim (X_1, \dots, X_{N-1}, X_N + u_3) \sim (X_1, \dots, X_{N-1}, X_N + u_4) \quad (3.21)$$

for  $u_3 = (m, 0)$  and  $u_4 = (-n, \frac{N}{m})$ . Hence the number of non-equivalent configurations is the index of the lattice  $\mathbb{Z}^2$  (thought off as corresponding to the last entry  $X_N$  in the extremum in its reduced form) in the lattice  $\bigoplus_{\alpha=1}^4 u_\alpha \mathbb{Z}$ . This index is given by the greatest

common divisor of the determinants of all pairs of vectors  $(u_\alpha, u_\beta)$  for  $1 \leq \alpha < \beta \leq 4$ .<sup>8</sup> The result is

$$\begin{aligned} \left[ \mathbb{Z}^2 : \bigoplus_{\alpha=1}^4 u_\alpha \mathbb{Z} \right] &= \gcd \left( N, 0, N \frac{d}{m}, N \frac{m}{d}, N \left( \frac{t}{m} + \frac{n}{d} \right), N \right) \\ &= \gcd \left( N \frac{d}{m}, N \frac{m}{d}, N \left( \frac{t}{m} + \frac{n}{d} \right) \right). \end{aligned} \quad (3.23)$$

We used the fact that a divisor of  $N \frac{d}{m}$  and  $N \frac{m}{d}$  is necessarily a divisor of  $N$ . Finally, we obtain a third formula for the number of vacua, based on the count of inequivalent solutions to the effective superpotential:

$$I^{\mathcal{N}=1^*}(N, m, n) = \sum_{d|N} \sum_{t=0}^{d-1} \gcd \left( N \frac{d}{m}, N \frac{m}{d}, N \left( \frac{t}{m} + \frac{n}{d} \right) \right). \quad (3.24)$$

This gives the multiplicity assigned to all sublattices of index  $N$ , which are labelled by  $(d, t)$ . In other words, if we draw figure 1 for algebra  $\mathfrak{su}(N)$ , in the box corresponding to column  $(d, t)$  and line  $SU(N)/\mathbb{Z}_m$ , there will be  $\gcd \left( N \frac{d}{m}, N \frac{m}{d}, N \left( \frac{t}{m} + \frac{n}{d} \right) \right)$  inequivalent lattices.

**Equivalence of the formulas.** No matter how we slice the index, the total tally should remain the same. Thus, we must show that the index (3.24) obtained through the exact superpotential approach is identical to the count (3.7) in the semi-classical analysis. This represents a non-trivial consistency check of the validity of our formulas. The proof involves more arithmetical lemmas that we relegate to appendix B.4. We first use the fact that

$$\gcd \left( N \frac{d}{m}, N \frac{m}{d}, N \left( \frac{t}{m} + \frac{n}{d} \right) \right) = \frac{N}{\text{lcm}(m, d)} \gcd \left( d, m, \frac{td + nm}{\gcd(d, m)} \right) \quad (3.25)$$

to rewrite (3.24) as

$$I^{\mathcal{N}=1^*}(N, m, n) = \frac{N}{m} \sum_{d|N} \sum_{t=1}^{\gcd(d, m)} \gcd \left( d, m, \frac{td + nm}{\gcd(d, m)} \right). \quad (3.26)$$

We introduce the shorthand  $\delta = \gcd(d, m)$ ,  $d' = \frac{d}{\delta}$  and  $m' = \frac{m}{\delta}$ , so that  $\gcd(d', m') = 1$ . We moreover define the cyclically ordered sequence  $D_a(\delta, d') = [\gcd(\delta, td' + a)]_{t \in \mathbb{Z}_\delta}$ . The index (3.24) becomes

$$I^{\mathcal{N}=1^*}(N, m, n) = \frac{N}{m} \sum_{d|N} \sum_{t=1}^{\delta} \gcd(\delta, td' + nm') = \frac{N}{m} \sum_{d|N} \sum_{x \in D_{nm'}(\delta, d')} x. \quad (3.27)$$

---

<sup>8</sup>Indeed, consider a rank  $n$  family  $(u_\alpha)_{\alpha=1, \dots, k}$  of vectors in  $\mathbb{Z}^n$ , with  $k \geq n$ . Let  $L$  be the sublattice of  $\mathbb{Z}^n$  generated by this family. The Smith normal form of the matrix formed by the list of vectors is  $\text{diag}(e_1, \dots, e_n)$  where  $e_1 \times \dots \times e_i$  is the greatest common divisor of all  $i \times i$  minors of the matrix, for  $i \leq n$ . We then have the equivalence

$$\frac{\mathbb{Z}^n}{L} \cong \bigoplus_{\alpha=1}^n \frac{\mathbb{Z}}{e_\alpha \mathbb{Z}}. \quad (3.22)$$

The index of  $\mathbb{Z}^n$  in this lattice is  $\prod_{i=1}^n e_i$ , which is equal to the determinant of all  $n \times n$  minors. This result also provides a basis of generators.

We must now refer to Lemma B.2 that shows that  $(\delta, nm')$ , which manifestly belongs to the sequence  $D_{nm'}(\delta, d')$ , is also an element of  $D_n(\delta, d')$ . From Lemma B.3 we then deduce that these two sequences are equal. We conclude that

$$I^{\mathcal{N}=1^*}(N, m, n) = \frac{N}{m} \sum_{d|N} \sum_{x \in D_n(\delta, d')} x = \frac{N}{m} \sum_{d|N} \sum_{t=1}^{\delta} \gcd(\delta, td' + n), \quad (3.28)$$

which is exactly equation (3.7). The arithmetic sticks.

## 4 Conclusions

We completed the table of indices of pure  $\mathcal{N} = 1$  Yang-Mills theories on a circle following [9]. Using the result for the  $\mathfrak{su}(n)$  algebra, we tallied the number of massive vacua of  $\mathcal{N} = 1^*$  gauge theories with  $A$ -type gauge algebra compactified on a circle, and demonstrated consistency with the duality of the parent  $\mathcal{N} = 4$  theory. It would be interesting to compute the supersymmetric index of  $\mathcal{N} = 1^*$  theories for all classical gauge algebras, for any choice of gauge group and spectrum of line operators, and any pick of twisted boundary conditions [19, 20]. The main ingredients will again be the supersymmetric index of pure  $\mathcal{N} = 1$  [9], the analysis of semi-classical solutions for the adjoint scalar fields, as well as the centralizer, including discrete factors [14, 16, 17]. The semi-direct product nature of the discrete part of the centralizers poses a hurdle — it can be jumped.

## Acknowledgments

We would like to acknowledge support from the grant ANR-13-BS05-0001, and from the École Polytechnique and the École Nationale Supérieure des Mines de Paris.

## A Supersymmetric indices of pure $\mathcal{N} = 1$ Yang-Mills theories

In this appendix, we assemble and complete the list of the number of vacua for pure  $\mathcal{N} = 1$  super Yang-Mills theories compactified on a circle. We follow the notation and logic of [9], to which we must refer for definitions and details. The theories with gauge algebras  $\mathfrak{b}$  and  $\mathfrak{c}$  as well as  $\mathfrak{d}_{N \text{ odd}}$  were entirely treated in [9], and we copied the results in table 2.

The cases of Lie algebra  $\mathfrak{g}_2, \mathfrak{f}_4$  and  $\mathfrak{e}_8$  are trivial since the adjoint group equals the covering group. Thus, we only need to complete the calculation for  $\mathfrak{a}_{N-1}$ , which is done in section 2, and the algebras  $\mathfrak{d}_{N \text{ even}}, \mathfrak{e}_6$  and  $\mathfrak{e}_7$ .

For the case  $\mathfrak{d}_{N \text{ even}}$ , the hypothesis is that there is a vacuum in which purely magnetic monopoles condense. The reasoning is standard, based on the identification of classes of vacua transforming into each other under the global symmetry group, and the Witten effect determining the spectrum of line operators in inequivalent vacua [9]. There is a laundry list of cases to go through, and the results are stacked in table 2. We provide example calculations below. For the exceptional groups, we divide the vacua into three groups of 4 for  $(E_6/\mathbb{Z}_3)_n$ , of which one group triples in degeneracy upon compactification, much as for the  $(\text{SU}(3)/\mathbb{Z}_3)_n$  theory, and into two groups of 9 for  $(E_7/\mathbb{Z}_2)_n$ , of which one group

Algebra	Theory	On $\mathbb{R}^4$	On $\mathbb{R}^3 \times S^1$
$\mathfrak{a}_{N-1}$	$(\mathrm{SU}(N)/\mathbb{Z}_m)_n$	$N$	$I^{N=1}(N, m, n)$
$\mathfrak{b}_{N \geq 2}$	$\mathrm{Spin}(2N+1)$ $\mathrm{SO}(2N+1)_+$ $\mathrm{SO}(2N+1)_-$	$2N-1$	$2N-1$ $2(2N-1)$ $2N-1$
$\mathfrak{c}_{N \geq 2}$	$\mathrm{Sp}(2N)$ $(\mathrm{Sp}(2N)/\mathbb{Z}_2)_+$ $(\mathrm{Sp}(2N)/\mathbb{Z}_2)_-$	$N+1$	$N+1$ $\begin{cases} 2(N+1) & \text{for even } N \\ \frac{3}{2}(N+1) & \text{for odd } N \end{cases}$ $\begin{cases} N+1 & \text{for even } N \\ \frac{3}{2}(N+1) & \text{for odd } N \end{cases}$
$\mathfrak{d}_{N \geq 3}$	$\mathrm{Spin}(2N)$ $\mathrm{SO}(2N)_+$ $\mathrm{SO}(2N)_-$	$2(N-1)$	$2(N-1)$ $4(N-1)$ $2(N-1)$
$\mathfrak{d}_{N \text{ odd}}$	$(\mathrm{Spin}(2N)/\mathbb{Z}_4)_n$	$2(N-1)$	$4(N-1)$
$\mathfrak{d}_{N \equiv 2 \pmod{4}}$	$\mathrm{Sc}(2N)_\pm$ and $\mathrm{Ss}(2N)_\pm$ $(\mathrm{SO}(2N)/\mathbb{Z}_2)_{00}^{00}$ $(\mathrm{SO}(2N)/\mathbb{Z}_2)_{11}^{11}$ $(\mathrm{SO}(2N)/\mathbb{Z}_2)_{00}^{10}$ $(\mathrm{SO}(2N)/\mathbb{Z}_2)_{11}^{01}$	$2(N-1)$	$3(N-1)$ $5(N-1)$ $3(N-1)$ $4(N-1)$ $2(N-1)$
$\mathfrak{d}_{N \equiv 0 \pmod{4}}$	$\mathrm{Sc}(2N)_+$ and $\mathrm{Ss}(2N)_+$ $\mathrm{Sc}(2N)_-$ and $\mathrm{Ss}(2N)_-$ $(\mathrm{SO}(2N)/\mathbb{Z}_2)_{00}^{00}$ $(\mathrm{SO}(2N)/\mathbb{Z}_2)_{11}^{11}$ $(\mathrm{SO}(2N)/\mathbb{Z}_2)_{00}^{01}$ $(\mathrm{SO}(2N)/\mathbb{Z}_2)_{10}^{00}$	$2(N-1)$	$4(N-1)$ $2(N-1)$ $5(N-1)$ $3(N-1)$ $3(N-1)$ $3(N-1)$
$\mathfrak{e}_6$	$E_6$ $(E_6/\mathbb{Z}_3)_n$	$12$	$12$ $20$
$\mathfrak{e}_7$	$E_7$ $(E_7/\mathbb{Z}_2)_n$	$18$	$18$ $27$
$\mathfrak{e}_8$	$E_8$	$30$	$30$
$\mathfrak{f}_4$	$F_4$	$9$	$9$
$\mathfrak{g}_2$	$G_2$	$4$	$4$

**Table 2.** The Pure  $\mathcal{N} = 1$  Indices on a Circle. The notations are as in [9].

doubles in degeneracy, similarly to what happens for  $(\text{SU}(2)/\mathbb{Z}_2)_n$ . This leads to a total of  $3 \times 4 + 4 + 4 = 20$  and  $2 \times 9 + 9$  vacua respectively.

To illustrate the inner workings of the added entries in table 2, we provide details of their calculation in the example of  $\mathfrak{d}_{N \equiv 0 \pmod 4}$ . The algebra  $\mathfrak{d}_{N \equiv 2 \pmod 4}$  can be treated similarly. When  $N$  is even, the center of the covering group  $\text{Spin}(2N)$  is  $\mathbb{Z}_2^S \times \mathbb{Z}_2^C$ , and we will compute the index of the pure  $\mathcal{N} = 1$  theories with gauge group  $\text{Spin}(2N)/\mathbb{Z}_2^C = \text{Sc}(2N)$  and  $\text{Spin}(2N)/(\mathbb{Z}_2^S \times \mathbb{Z}_2^C) = \text{SO}(2N)/\mathbb{Z}_2$  on a circle. The  $\text{Ss}(2N)$  theory is related to the  $\text{Sc}(2N)$  theory by the action of the outer automorphism, and the other groups are covered in [9]. A line operator with electric charge  $(z_{e,S}, z_{e,C})$  and magnetic charge  $(z_{m,S}, z_{m,C})$  is labelled by the element  $(z_{e,S}, z_{e,C}; z_{m,S}, z_{m,C})$  in  $\mathbb{Z}_2^4$ . Equivalently, we can label the line by equivalence classes of weights  $([\lambda_e]; [\lambda_m])$  where

$$[\lambda_e], [\lambda_m] \in \{[0] = (0, 0), [\lambda_S] = (1, 0), [\lambda_C] = (0, 1), [\lambda_V] = (1, 1)\} = \mathbb{Z}_2^2. \tag{A.1}$$

From now on, we drop the square brackets. Two line operators are mutually local if and only if

$$z_{e,S} z'_{m,C} - z_{m,C} z'_{e,S} \equiv z_{e,C} z'_{m,S} - z_{m,S} z'_{e,C} \pmod 2, \tag{A.2}$$

and, combined with the fact that purely electric lines have electric charges in the weight lattice of the gauge group, and completeness, this determines the possible line operator spectra [9].

We work under the assumption that there exists a vacuum where all the particles that condense are purely magnetic. The  $2N - 2$  vacua of the  $\mathfrak{so}(2N)$  theories on  $\mathbb{R}^4$  are divided into two classes. We have  $N - 1$  vacua which are related by the global discrete symmetry group to a vacuum where particles with purely magnetic charges in the set  $\mathcal{C}_1 = \{(0; \alpha_i)\}_{i=1, \dots, N}$  condense, where  $\alpha_i$  generate a maximal rank sublattice of the root lattice. There are also  $N - 1$  vacua related to a vacuum where particles with equal electric and magnetic charges  $\mathcal{C}_2 = \{(\alpha_i; \alpha_i)\}_{i=1, \dots, N}$  condense. We will suppose that the charges  $\alpha_i$  correspond to simple roots of the Lie algebra. These hypotheses are supported by the physics of  $\mathcal{N} = 2$  supersymmetric gauge theories upon breaking to  $\mathcal{N} = 1$  by mass deformation.

Now, a line operator of charge  $\mathcal{L} = (\lambda_e; \lambda_m)$  in a vacuum with condensates of charges  $\mathcal{C} = \{(\alpha_{e,i}; \alpha_{m,i})\}_{i=1, \dots, N}$  on  $\mathbb{R}^4$  indicates an unbroken magnetic gauge symmetry if and only if

$$\{\lambda_e \cdot \alpha_{m,i} - \lambda_m \cdot \alpha_{e,i}\}_{i=1, \dots, N} = \{0, \dots, 0\} \pmod 2. \tag{A.3}$$

When this is the case, the line follows a perimeter law. In a theory with a given spectrum  $\{\mathcal{L}\}$  of line operators, the unbroken magnetic gauge group is therefore  $\mathbb{Z}_2^{p(\mathcal{C}, \{\mathcal{L}\})}$  where  $p(\mathcal{C}, \{\mathcal{L}\})$  is the rank of the lattice of charges of line operators that follow a perimeter law. Upon compactification, such a vacuum leads to a degeneracy equal to the cardinal number of this unbroken discrete group. Therefore the number of vacua on  $\mathbb{R}^3 \times S^1$  is

$$\frac{2N - 2}{2} \sum_{k=1}^2 2^{p(\mathcal{C}_k, \{\mathcal{L}\})}, \tag{A.4}$$

where the sum runs on the two vacua related by the transformation  $\theta \rightarrow \theta + 2\pi$ . The calculation is described explicitly in table 3.

Theory	Lines $\mathcal{L}$	$p(\mathcal{C}_1, \{\mathcal{L}\})$		$p(\mathcal{C}_2, \{\mathcal{L}\})$		Total
$\text{Sc}(2N)_+$	$(\lambda_S, 0)$	A	1	A	1	$4(N-1)$
	$(0, \lambda_S)$	P				
	$(\lambda_S, \lambda_S)$	A				
$\text{Sc}(2N)_-$	$(\lambda_S, 0)$	A	0	A	0	$2(N-1)$
	$(\lambda_C, \lambda_S)$	A				
	$(\lambda_V, \lambda_S)$	A				
$(\text{SO}(2N)/\mathbb{Z}_2)_{00}^{00}$	$(0, \lambda_S)$	P	2	A	0	$5(N-1)$
	$(0, \lambda_C)$	P				
	$(0, \lambda_V)$	P				
$(\text{SO}(2N)/\mathbb{Z}_2)_{11}^{11}$	$(\lambda_V, \lambda_S)$	A	1	A	0	$3(N-1)$
	$(\lambda_V, \lambda_C)$	A				
	$(0, \lambda_V)$	P				
$(\text{SO}(2N)/\mathbb{Z}_2)_{00}^{01}$	$(\lambda_C, \lambda_S)$	A	1	A	0	$3(N-1)$
	$(0, \lambda_C)$	P				
	$(\lambda_C, \lambda_V)$	A				
$(\text{SO}(2N)/\mathbb{Z}_2)_{10}^{00}$	$(0, \lambda_S)$	P	1	A	0	$3(N-1)$
	$(\lambda_S, \lambda_C)$	A				
	$(\lambda_S, \lambda_V)$	A				

**Table 3.** The computation of the number of vacua in the compactified  $\mathfrak{d}_{N \equiv 0 \pmod 4}$  theories. The letters A and P indicate that the line follows an area or perimeter law, respectively.

## B The details and the arithmetic

This appendix contains the inner workings of various technical reasonings in the bulk of the paper. In appendix B.1, we present a more detailed analysis of the unbroken gauge group argued for in subsection 3.1. In subsections B.2, B.3 and B.4, we provide proofs of useful arithmetic identities.

### B.1 The unbroken gauge group

Let  $d$  be a divisor of  $N$ , and  $k = N/d$ . Let  $m$  be a divisor of  $N$ . In this subsection we compute in more technical detail the residual gauge group

$$H_{\mathbb{C}} = S \left( \text{GL}(d)_{\Delta}^k \right) \cap G_{\mathbb{C}}. \tag{B.1}$$

with  $G_{\mathbb{C}} = \text{SL}(n, \mathbb{C})/\mathbb{Z}_m$ . We first note that

$$H_{\mathbb{C}} = \left[ S \left( \text{GL}(d)_{\Delta}^k \right) \right] / \mathbb{Z}_m. \tag{B.2}$$

Consider the map  $\psi$

$$\psi : \text{SL}(d) \times \mathbb{Z}_k \rightarrow H_{\mathbb{C}} : \tag{B.3}$$

$$(A, l) \mapsto e^{2\pi i l/N} \{1, e^{2\pi i/m}, \dots, e^{2\pi i(m-1)/m}\} \text{diag}(A, \dots, A), \tag{B.4}$$



where we map into elements of the set  $H_{\mathbb{C}}$ , which are equivalence classes. Let us note various properties of this group homomorphism:

- It is surjective. Indeed, consider a representative  $\text{diag}(B, \dots, B)$  of a  $\mathbb{Z}_m$  equivalence class in  $S((\text{GL}(d))_{\Delta}^k)$ . We have  $\det B^k = 1$ , so there exists  $l \in \mathbb{Z}_k$  such that  $\det B = e^{2\pi il/k}$ . Define  $A = e^{-2\pi il/N} B$ . Then  $\det A = e^{-2\pi il/k} \det B = 1$ .
- We have  $\text{Ker}\psi \cong \mathbb{Z}_m$ . This isomorphism is given explicitly by

$$s \mapsto \left( A = \exp 2\pi i \left( \frac{s}{m} - \frac{l}{N} \right) 1_{d \times d}, l = s \frac{N}{m} \pmod{k} \right). \quad (\text{B.5})$$

By the isomorphism theorem, we have

$$H_{\mathbb{C}} \cong \frac{\text{SL}(d) \times \mathbb{Z}_k}{\mathbb{Z}_m}. \quad (\text{B.6})$$

We know how  $\mathbb{Z}_m$  acts on  $\text{SL}(d) \times \mathbb{Z}_k$  thanks to equation (B.5). The action is the same as the action of  $\mathbb{Z}_{\text{gcd}(d,m)} \times \mathbb{Z}_{m/\text{gcd}(d,m)}$ . Hence we can write

$$H_{\mathbb{C}} \cong \frac{\text{SL}(d)}{\mathbb{Z}_{\text{gcd}(d,m)}} \times \frac{\mathbb{Z}_k}{\mathbb{Z}_{m/\text{gcd}(d,m)}} = \frac{\text{SL}(d)}{\mathbb{Z}_{\text{gcd}(d,m)}} \times \mathbb{Z}_{N/\text{lcm}(d,m)}. \quad (\text{B.7})$$

This detailed technical analysis proves the conclusion drawn in subsection 3.1.

## B.2 A warm-up for $S$ -duality

As a consequence of  $S$ -duality, the indices (3.8) and (3.9) of the  $\mathcal{N} = 1^*$  theories  $\text{SU}(N)$  and  $(\text{SU}(N)/\mathbb{Z}_N)_0$  have to be equal. To prove the equality, we exploit Euler's totient function  $\varphi(n)$  which counts the number of integers  $1 \leq k \leq n$  that are coprime to  $n$ . For  $d$  a divisor of  $n$ , we have

$$\varphi\left(\frac{n}{d}\right) = |\{1 \leq k \leq n \mid \text{gcd}(k, n) = d\}|. \quad (\text{B.8})$$

We then compute

$$\sum_{d|n} \varphi(d) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{k=1}^n \delta_{\text{gcd}(k,n)=d} = \sum_{k=1}^n \sum_{d|n} \delta_{\text{gcd}(k,n)=d} = \sum_{k=1}^n 1 = n, \quad (\text{B.9})$$

and similarly

$$\sum_{d|n} d\varphi\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{k=1}^n d\delta_{\text{gcd}(k,n)=d} = \sum_{k=1}^n \sum_{d|n} d\delta_{\text{gcd}(k,n)=d} = \sum_{k=1}^n \text{gcd}(k, n). \quad (\text{B.10})$$

Now we can combine the two equalities to prove the desired identity:

$$\begin{aligned} \sum_{n|N} \sum_{k=1}^n \text{gcd}(k, n) &= \sum_{n|N} \sum_{d|n} d\varphi\left(\frac{n}{d}\right) = \sum_{d|N} d \sum_{d|n|N} \varphi\left(\frac{n}{d}\right) \\ &= \sum_{d|N} d \sum_{n'|\frac{N}{d}} \varphi(n') = \sum_{d|N} d \frac{N}{d} = N\sigma_0(N). \end{aligned} \quad (\text{B.11})$$

This finishes our warm-up example for the proof of  $S$ -duality in the generic case in subsections 3.2 and 3.3.

### B.3 A sum of greatest common divisors

This subsection is devoted to the derivation of the formula (3.11). This is a particular case of the identity [21]

$$\sum_{s=1}^n \gcd(n, f(s)) = n \sum_{d|n} \frac{\varphi(d)}{d} \rho(d, f), \quad (\text{B.12})$$

where  $f$  is any polynomial with integer coefficients, and  $\rho(d, f)$  is the number of solutions of the equation  $f(s) = 0$  in  $\mathbb{Z}_d$ . Since we only need a small subset of the identities proven in [21], we limit the proof of [21] to our simpler context. The essential ingredients are the Möbius function identity and the exchange of two sums over divisors:

$$\begin{aligned} \sum_{s=1}^n \gcd(n, f(s)) &= \sum_{d|n} d \sum_{s=1}^n \delta[\gcd(f(s), n) = d] \\ &= \sum_{d|n} d \sum_{s=1}^n \sum_{e|\gcd(\frac{f(s)}{d}, \frac{n}{d})} \mu(e) \end{aligned} \quad (\text{B.13})$$

$$\begin{aligned} &= \sum_{d|n} d \sum_{e|\frac{n}{d}} \sum_{s=1}^n \mu(e) \delta[de|f(s)] \\ &= \sum_{d|n} d \sum_{e|\frac{n}{d}} \mu(e) \rho(de, f) \frac{n}{de} \\ &= \sum_{d|n} d \sum_{d|u|n} \mu\left(\frac{u}{d}\right) \rho(u, f) \frac{n}{u} \\ &= \sum_{u|n} \rho(u, f) \frac{n}{u} \sum_{d|u} d \mu\left(\frac{u}{d}\right) \\ &= \sum_{u|n} \rho(u, f) \frac{n}{u} \varphi(u). \end{aligned} \quad (\text{B.14})$$

We use the Möbius function identity in steps (B.13) and (B.14) respectively. To recuperate the formula (3.11), we analyze the number of solutions  $s$  to the Diophantine equation  $as + b = 0$  modulo  $n$ . If the equation has a solution, then there exist integers  $s$  and  $r$  such that  $as + b = rn$ , and therefore  $\gcd(a, n) | b$ . If this condition is not fulfilled, the equation has no solution. If it is, then we have  $\gcd(a, n)$  solutions. Thus, formula (B.12) implies the desired formula (3.11).

### B.4 Auxiliary lemmas

**Lemma B.1.** *Let  $v$  and  $d'$  be two integers such that  $\gcd(v, d') = 1$  and let  $\delta'$  be any integer. Then there exists  $k \in \mathbb{Z}$  such that  $\gcd(\delta', v - d'k) = 1$ .*

*Proof.* Let  $P$  be the set of prime numbers that divide  $\delta'$  but that do not divide  $v$  nor  $d'$ . We now define  $k = \prod_{p \in P} p$ . Let  $p$  be a prime that divides  $\delta'$ . There are three possibilities:

- If  $p$  divides  $v$ , then  $p \notin P$  so  $p$  doesn't divide  $k$ . It doesn't divide  $d'$  either because  $\gcd(v, d') = 1$ . Therefore  $p$  does not divide  $v - d'k$ , and does not divide  $\gcd(\delta', v - d'k)$ .

- If  $p$  divides  $d'$ , then it does not divide  $v$ , nor  $v - d'k$ , nor  $\gcd(\delta', v - d'k)$ .
- The last possibility is that  $p \in P$ . But then  $p$  does not divide  $v$ , and does not divide  $\gcd(\delta', v - d'k)$ .

We see that no prime can divide  $\gcd(\delta', v - d'k)$ , so this number must be equal to one.  $\square$

**Lemma B.2.** *Let  $\delta \in \mathbb{N}^*$ , let  $d'$  and  $m'$  be integers such that  $(d', m') = 1$  and let  $n \in \mathbb{Z}$ . Then there exists  $a \in \mathbb{Z}$  such that*

$$\gcd(\delta, ad' + n) = \gcd(\delta, nm'). \quad (\text{B.15})$$

*Proof.* We use Bézout's theorem to introduce  $(u, v) \in \mathbb{Z}^2$  such that  $ud' + vm' = 1$ . We also define  $\delta' = \frac{\delta}{(\delta, nm')}$ . Note that Bézout's theorem asserts that  $\gcd(v, d') = 1$ , so we can apply lemma B.1. Let  $k$  be the integer given by this lemma and write

$$1 = (u + m'k)d' + (v - d'k)m'. \quad (\text{B.16})$$

Then if we set  $a = -n(u + m'k)$ , we have

$$\begin{aligned} \gcd(\delta, ad' + n) &= \gcd(\delta, ad' + n(u + m'k)d' + (v - d'k)nm') \\ &= \gcd(\delta, (v - d'k)nm') \\ &= \gcd(\delta, nm') \gcd(\delta', v - d'k) \\ &= \gcd(\delta, nm'). \end{aligned} \quad (\text{B.17})$$

$\square$

**Lemma B.3.** *Let  $\delta \in \mathbb{N}^*$  and  $d \in \mathbb{N}^*$ . For  $a \in \mathbb{Z}_d$ , define the cyclic ordered sequence*

$$D_a(\delta, d) = [\gcd(\delta, a + dt)]_{t \in \mathbb{Z}_\delta}. \quad (\text{B.18})$$

*If the sequences  $D_a(\delta, d)$  and  $D_b(\delta, d)$  have an element in common, then they are equal as cyclic ordered sequences.*

*Proof.* Let us call  $\mathcal{P}(\delta, d)$  the property that we want to prove. Let us first show that it is sufficient to prove  $\mathcal{P}(\delta, d)$  for  $d$  a divisor of  $\delta$ . The additive group  $d\mathbb{Z}/\delta\mathbb{Z}$  is isomorphic to the group  $d_1\mathbb{Z}/\delta\mathbb{Z}$  where  $d_1 = \gcd(\delta, d)$ . This group isomorphism gives rise to a reshuffling of numbers inside  $\mathbb{Z}_\delta$ , determined by  $d$  and  $d_1$ . The fact that the reshuffling is common between the two sequences implies that we can prove the lemma for  $\gcd(\delta, \cdot)$  applied to the sets  $\{a + d_1t | t \in \mathbb{Z}\}$  and  $\{b + d_1t | t \in \mathbb{Z}\}$ .

Now we prove by induction on  $\delta$  that  $\forall d | \delta, \mathcal{P}(\delta, d)$ . This is obvious for  $\delta = 1$ . Consider then  $\delta > 1$ . The property  $\mathcal{P}(\delta, 1)$  is clear, so we choose a divisor  $d > 1$ , and define  $k = \delta/d < \delta$ . Let  $a, b \in \mathbb{Z}_d$  such that  $D_a(\delta, d)$  and  $D_b(\delta, d)$  have an element in common. With the notation  $a_1 = \gcd(\delta, d, a) = \gcd(d, a)$ , we have that

$$\gcd(\delta, a + dt) = a_1 \gcd\left(k \frac{d}{a_1}, \frac{a}{a_1} + \frac{d}{a_1}t\right) = a_1 \gcd\left(k, \frac{a}{a_1} + \frac{d}{a_1}t\right). \quad (\text{B.19})$$

We used the fact that  $a/a_1$  is coprime with  $d/a_1$  in the last equality.

But we know that there exist  $t, t'$  such that  $(kd, a + dt) = (kd, b + dt')$ . Then any divisor of  $d$  and  $a$  is a divisor of  $(kd, a + dt) = (kd, b + dt')$  and therefore also a divisor of  $b$ . This proves that  $a_1|b_1 = \gcd(d, b)$ . Similarly,  $b_1|a_1$ . Thus,  $a_1 = b_1$ , and we deduce that

$$\gcd(\delta, b + dt) = b_1 \gcd\left(k, \frac{b}{b_1} + \frac{d}{b_1}t\right) = a_1 \gcd\left(k, \frac{b}{a_1} + \frac{d}{a_1}t\right). \quad (\text{B.20})$$

The sequences in the right-hand sides of (B.19) and (B.20) have an element in common, and using  $\mathcal{P}(k, d/a_1)$ , they are equal as cyclic sequences. Hence the same holds for the left-hand sides, proving the property  $\mathcal{P}(\delta, d)$  and the lemma.  $\square$

**Open Access.** This article is distributed under the terms of the Creative Commons Attribution License ([CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/)), which permits any use, distribution and reproduction in any medium, provided the original author(s) and source are credited.

## References

- [1] E. Witten, *Constraints on Supersymmetry Breaking*, *Nucl. Phys. B* **202** (1982) 253 [[INSPIRE](#)].
- [2] E. Witten, *Toroidal compactification without vector structure*, *JHEP* **02** (1998) 006 [[hep-th/9712028](#)] [[INSPIRE](#)].
- [3] A. Keurentjes, A. Rosly and A.V. Smilga, *Isolated vacua in supersymmetric Yang-Mills theories*, *Phys. Rev. D* **58** (1998) 081701 [[hep-th/9805183](#)] [[INSPIRE](#)].
- [4] A. Keurentjes, *Nontrivial flat connections on the 3 torus I:  $G_2$  and the orthogonal groups*, *JHEP* **05** (1999) 001 [[hep-th/9901154](#)] [[INSPIRE](#)].
- [5] A. Keurentjes, *Nontrivial flat connections on the three torus. 2. The Exceptional groups  $F_4$  and  $E_6, E_7, E_8$* , *JHEP* **05** (1999) 014 [[hep-th/9902186](#)] [[INSPIRE](#)].
- [6] V.G. Kac and A.V. Smilga, *Vacuum structure in supersymmetric Yang-Mills theories with any gauge group*, [hep-th/9902029](#) [[INSPIRE](#)].
- [7] A. Borel, R. Friedman and J.W. Morgan, *Almost commuting elements in compact Lie groups*, *Memoirs of the American Mathematical Society*, Volume 157, Issue 747, AMS (2002), [[math/9907007](#)] [[INSPIRE](#)].
- [8] E. Witten, *Supersymmetric index in four-dimensional gauge theories*, *Adv. Theor. Math. Phys.* **5** (2002) 841 [[hep-th/0006010](#)] [[INSPIRE](#)].
- [9] O. Aharony, N. Seiberg and Y. Tachikawa, *Reading between the lines of four-dimensional gauge theories*, *JHEP* **08** (2013) 115 [[arXiv:1305.0318](#)] [[INSPIRE](#)].
- [10] O. Aharony, S.S. Razamat, N. Seiberg and B. Willett, *3d dualities from 4d dualities for orthogonal groups*, *JHEP* **08** (2013) 099 [[arXiv:1307.0511](#)] [[INSPIRE](#)].
- [11] M.M. Anber and E. Poppitz, *On the global structure of deformed Yang-Mills theory and  $QCD(adj)$  on  $\mathbb{R}^3 \times \mathbb{S}^1$* , *JHEP* **10** (2015) 051 [[arXiv:1508.00910](#)] [[INSPIRE](#)].
- [12] R. Donagi and E. Witten, *Supersymmetric Yang-Mills theory and integrable systems*, *Nucl. Phys. B* **460** (1996) 299 [[hep-th/9510101](#)] [[INSPIRE](#)].
- [13] N. Dorey, *An Elliptic superpotential for softly broken  $N = 4$  supersymmetric Yang-Mills theory*, *JHEP* **07** (1999) 021 [[hep-th/9906011](#)] [[INSPIRE](#)].

- [14] A. Bourget and J. Troost, *Counting the Massive Vacua of  $N = 1^*$  Super Yang-Mills Theory*, *JHEP* **08** (2015) 106 [[arXiv:1506.03222](#)] [[INSPIRE](#)].
- [15] D. Collingwood and W. McGovern, *Nilpotent Orbits In Semisimple Lie Algebra*, CRC Press (1993).
- [16] A. Bourget and J. Troost, *Duality and modularity in elliptic integrable systems and vacua of  $\mathcal{N} = 1^*$  gauge theories*, *JHEP* **04** (2015) 128 [[arXiv:1501.05074](#)] [[INSPIRE](#)].
- [17] A. Bourget and J. Troost, *On the  $\mathcal{N} = 1^*$  gauge theory on a circle and elliptic integrable systems*, *JHEP* **01** (2016) 097 [[arXiv:1511.03116](#)] [[INSPIRE](#)].
- [18] O. Aharony, N. Dorey and S.P. Kumar, *New modular invariance in the  $N = 1^*$  theory, operator mixings and supergravity singularities*, *JHEP* **06** (2000) 026 [[hep-th/0006008](#)] [[INSPIRE](#)].
- [19] A. Hanany and J. Troost, *Orientifold planes, affine algebras and magnetic monopoles*, *JHEP* **08** (2001) 021 [[hep-th/0107153](#)] [[INSPIRE](#)].
- [20] S. Kim, K.-M. Lee, H.-U. Yee and P. Yi, *The  $N = 1^*$  theories on  $R^{(1+2)} \times S^1$  with twisted boundary conditions*, *JHEP* **08** (2004) 040 [[hep-th/0403076](#)] [[INSPIRE](#)].
- [21] J. Chidambaraswamy and R. Sitaramachandrarao, *Asymptotic Results for a Class of Arithmetical Functions*, *Mh. Math.* **99** (1985) 19.