Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Geometry and Physics 52 (2004) 284–297

JOURNAL OF GEOMETRY AND PHYSICS

www.elsevier.com/locate/jgp

Integrality of open instantons numbers

Daniel B. Grünberg*

KdV Institute, University of Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands

Received 14 May 2003; accepted 18 March 2004
Available online 27 April 2004

Abstract

We prove the integrality of the open instanton numbers in two examples of counting holomorphic disks on local Calabi–Yau three-folds: the resolved conifold and the degenerate $\mathbf{P}^1 \times \mathbf{P}^1$. Given the B-model superpotential, we extract by hand all Gromow–Witten invariants in the expansion of the A-model superpotential. The proof of their integrality relies on enticing congruences of binomial coefficients modulo powers of a prime. We also derive an expression for the factorial $(p^k - 1)!$ modulo powers of the prime p. We generalise two theorems of elementary number theory, by Wolstenholme and Wilson.

JGP SC: Superstrings; Algebraic geometry

Keywords: Open instantons; Enumerative geometry; Gromow–Witten invariants; Integrality of BPS invariants; Wolstenholme and Wilson theorems

1. Introduction

Open string instantons are holomorphic maps from Riemann surfaces with boundaries to the CY_3 target space. It is understood that the boundaries of the instanton end on special Lagrangian submanifolds of the three-fold. In other words, we are interested in the problem of counting holomorphic disks with boundary on a Lagrangian submanifold.

Aganagic and Vafa [1] used Mirror Symmetry to determine these open string instantons: the B-model superpotential can be computed exactly and mapped to the A-model superpotential in the large volume limit of the CY_3. The latter cannot be computed exactly, but contains instanton corrections, i.e. holomorphic disks ending on "A-model branes" (also

* Tel.: +31-20-525-60-97; fax: +31-20-525-51-01.
E-mail address: grunberg@science.uva.nl (D.B. Grünberg).

0393-0440/$ – see front matter
doi:10.1016/j.geomphys.2004.03.004

called A-branes); comparison with the B-model superpotential allow us to determine the contribution of these instantons and their degeneracy.

The disk amplitude in the large volume limit (i.e. $e^v \to 0$), which—in the type II context—has the interpretation of superpotential corrections to $4d$ $N = 1$ susy, is expected to be of the form [2] (A-model superpotential):

$$W_A = \sum_{\substack{n\geq 1\\ k,m}} \frac{d_{k,m}}{n^2} q^{nk} y^{nm}, \tag{1}$$

where $q = e^{-t}$ and $y = e^v$ are the (exponentiated) closed and open string complexified Kähler classes, measuring respectively the volume of compact curves and holomorphic disks embedded in the three-fold. The coefficients $d_{k,m}$ are the numbers of primitive holomorphic disks labelled by the classes k and m—two vectors in the homologies H_2 of the three-fold and H_1 of the brane respectively.

The tables given in [1] exhibit the integrality of the coefficients $d_{k,m}$ for their two examples of three-folds: the resolved conifold and the degenerate $\mathbf{P}^1 \times \mathbf{P}^1$. The current paper proves this for all k, m by analytic means. We first Fourier expand the B-model superpotential [1] in q and y and equate it to (1), then we prove the integrality of $d_{k,m}$ by proceeding inductively on the greatest common divisor of k and m. We derive interesting congruences of binomial coefficients modulo powers of a prime.

This explicit method is only possible due to the simple nature of the mirror map: for $\mathbf{P}^1$ (both examples), the relation between t and $\hat{t}$ is rational: $q = \hat{q}/(1 + \hat{q})^2$.

The first four sections are a reminder of the method used in [1]; it rests on the equivalence of the A- and B-model under mirror symmetry. On one hand, the A-model string amplitude is re-interpreted in topological string theory as counting holomorphic maps from Riemann surfaces (with boundary) to the target space; on the other hand, the B-model amplitude is obtained via Chern–Simons reduction to the world-volume of the B-brane.

The last two sections and the mathematical Appendix A are the crux of the paper: we prove the integrality of the open instanton numbers in the examples of the resolved conifold $\mathcal{O}(-1) \times \mathcal{O}(-1) \to \mathbf{P}^1$ and of the degenerate $\mathbf{P}^1 \times \mathbf{P}^1$ (where one $\mathbf{P}^1$ gets infinite volume). Appendix A proves the following powerful congruences for a prime $p > 3$ and integers n, k, l:

$$\binom{np^l}{kp^l} \equiv \binom{np^{l-1}}{kp^{l-1}} \bmod p^{3l}, \qquad (p^k - 1)!' \equiv -1 \bmod p^l \quad (k \geq l).$$

These are generalisations of Wolstenholme's and Wilson's theorems, respectively.

2. The A-model

For the A-model, we consider a $U(1)$ linear sigma model, i.e. a complex Kähler manifold Y obtained by quotienting the hypersurface

$$L_Y := \left\{ \sum_{i=1}^{n} Q_i |\Phi^i|^2 = r^2 \right\} \tag{2}$$

of $\mathbb{C}^n$ by a $U(1)$ subgroup of the isometry group of $\mathbb{C}^n$. The charges Q_i are integers, and if they sum up to 0, Y is a complex $(n-1)$-dimensional CY manifold (non-compact, as the directions with negative charge are non-compact).

More generally, we view $\mathbb{C}^n$ as a torus fibration $T^n \to L$, where the base is just $\mathbb{R}^n$ parametrised by the $|\Phi^i|$. We can also consider a real k-dimensional subset L_Y of L given by $(n-k)$ equations (2) for $(n-k)$ sets of charges Q_i^a, and then divide the fibration by $U(1)^{n-k}$ to obtain a fibration $Y = (T^k \to L_Y)$ which is a complex k-dimensional non-compact CY manifold.

Note that the base L_Y is a Lagrangian submanifold of Y: since L is given by fixing values of the arguments θ^i of the complex variables Φ^i, the Kähler form $\omega = \sum_{i=1}^n d|\Phi^i|^2 \wedge d\theta^i$ vanishes on it. The base L_Y is our first example of a Dk-brane.

Other examples of Dk-branes are obtained by considering rational linear subspaces of L_Y, i.e. submanifolds $D^r \subset L_Y$ of real dimension $r \leq k$, given by $(k-r)$ constraints

$$\sum_{i=1}^n q_i^\alpha |\Phi^i|^2 = c^\alpha \tag{3}$$

with integers q_i^α, $\alpha = 1, \ldots, k-r$. Since the slope of D^r is rational, the $(k-r)$-dimensional subspace of the fibre T^k above any point of D^r and orthogonal—w.r.t. ω—to T_pD^r is itself a torus T^{k-r}. That is, we have a new Dk-brane given by the fibration $T^{k-r} \to D^r$. As a submanifold of Y, it is *special* Lagrangian iff $\sum_i q_i^\alpha = 0$. All these special Lagrangian submanifolds of Y are called A-branes.

3. The B-model

The mirror equation to (2) is

$$\prod_{i=1}^n y_i^{Q_i} = \mathrm{e}^{-t}, \tag{4}$$

where $t := r + i\theta$ is the complexified Kähler parameter, i.e. the Fayet–Iliopoulos term r of (2) combined with the $U(1)$ θ angle. The y_i are homogeneous coordinates for $\mathbf{P}^{n-1}$. When L_Y is given by a set of $(n-k)$ equations, (4) also consists of $(n-k)$ equations for different Kähler parameters t_a.

Note that (4) is not yet the equation of the mirror CY space. The B-model is a Landau–Ginsburg theory with superpotential

$$W(y_i) = \sum_{i=1}^n y_i,$$

in which $(n-k)$ of the complex variables y_i can be substituted by (4), leaving just k of them. The mirror CY space is compact or not according to whether we add or not a gauge-invariant superpotential term $PG(\phi_i)$ to the original theory. In the first case, the CY is given by an orbifold of the hypersurface $W(y_i) = 0$, thus $(k-2)$-dimensional. In the second case, it is given by $W(y_i) = xz$, where x, z are affine (and not projective!) coordinates giving rise to non-compact directions, thus k-dimensional. (Note that sometimes the y_i variables occurring in $W(y_i)$ are rescaled to new variables $\tilde{y}_i$ such that these appear with powers different from 1.)

As for the B-brane, the mirror of equation (3) is

$$\prod_{i=1}^{n} y_i^{q_i^\alpha} = \epsilon^\alpha \, \mathrm{e}^{-c^\alpha}, \qquad \alpha = 1, \ldots, k-r, \tag{5}$$

as a subspace of the mirror CY. We have allowed a phase ϵ^α to occur; in other words, we have complexified c^α. Thus the B-brane is a holomorphic submanifold of complex dimension $k-(k-r)=r$, i.e. it is a D($2r$)-brane, where r was the real dimension of the base of the A-brane.

4. Topological strings and Chern–Simons action

In order to extract instanton numbers from our description of A-branes and their mirror B-branes, we need an alternative way of computing the B-model superpotential. We find salvation in topological string theory, where the A-model string amplitude counts holomorphic maps from Riemann surfaces with boundary to the target space with the boundary ending on A-branes, while the B-model amplitude computes the holomorphic Chern–Simons action reduced to the world-volume of the B-brane. Hence it only works for the CY *three*-folds, i.e. from now on we restrict to $k=3$.

Since the A-model disk amplitude in the large volume limit computes corrections to the $4d$ $N=1$ superpotential, we can extract its instanton numbers from the B-model superpotential, i.e. from the classical action

$$W = \int_Y \Omega \wedge \mathrm{Tr}\left[A\bar{\partial}A + \frac{2}{3}A^3\right] \tag{6}$$

for a holomorphic $U(N)$ gauge field $A \in H^{0,1}(Y, \mathrm{adj}\, U(N))$.

We shall be interested in the cases where the B-brane is a D2-brane, i.e. a holomorphic curve $\mathcal{C}$; that is the case $r=1$ with r being the real dimension of the base of the A-brane. Then the components of the gauge field A are holomorphic sections of the normal bundle $N(\mathcal{C})$, call them s, and the reduced Chern–Simons action is

$$W(\mathcal{C}) = \int_{\mathcal{C}} \Omega_{ijz} s^i \bar{\partial}_{\bar{z}} s^j \, \mathrm{d}z \, \mathrm{d}\bar{z}, \tag{7}$$

which vanishes in the light of $\bar{\partial}_{\bar{z}} s^j(z) = 0$. This is clearly unattractive for our purposes. A way of obtaining a non-vanishing result is to consider the variation of the integral under holomorphic deformations of $\mathcal{C}$. This wound not vanish if we have obstructions to holomorphic deformations, such as boundary conditions for the B-brane at infinity.

This requires a non-compact B-brane $\mathcal{C}$, hence a non-compact mirror CY given by $\{W(y_i) = xz\}$ for $k=3$ homogeneous coordinates y_i. This equation reads $\{F(u,v) = xz\}$ for two affine complex variables u, v, say $y_1 = \mathrm{e}^u$, $y_2 = \mathrm{e}^v$. Since $r=1$, the B-brane is given by $k-1=2$ equations in the variables y_i, hence fixing $W(y_i)$ or $F(u,v)$ to a constant value. If this value is 0, the B-brane will split into two submanifolds $\{x = 0\}$ and $\{z = 0\}$ and hence deformations will be obstructed (as otherwise the brane would pick up a boundary) and the B-model superpotential $W(\mathcal{C})$ will not vanish, as desired.

Note that we can similarly obtain configurations where the A-brane will split into two: for instance, a charge $q = (1, -1, 0, \dots, 0)$ restricts the Lagrangian submanifold L_Y to $\{|\Phi_1|^2 - |\Phi_2|^2 = c\}$ and for vanishing c the A-brane will enter a phase where it splits into $\{\Phi_1 = \Phi_2\}$ and $\{\Phi_1 = -\Phi_2\}$.

To finish off the computation of the B-model Chern–Simons action, we fix the values of one of the affine parameters u, v of the B-brane at infinity to some constant value (say $v \to v_*$ for large $|z|$). This parameter v measures, on the A-model side, the size of the holomorphic disk ending on the brane. We then choose u and v as the two sections of the normal bundle $N(\mathcal{C})$. $\mathcal{C}$ itself is parametrised by z, and the last variable x parametrising the B-brane is set to 0. We write the holomorphic three-form as $\Omega = \mathrm{d}u\,\mathrm{d}v\,\mathrm{d}z/z$ and obtain for the above integral:

$$W(\mathcal{C}) = \int_{\mathcal{C}} \frac{\mathrm{d}z}{z} u \bar{\partial}_{\bar{z}} v \,\mathrm{d}\bar{z} = \int_{v_*}^{v} u \,\mathrm{d}v.$$

This has the form of an Abel–Jacobi map for the one-form $u\,\mathrm{d}v$ on the Riemann surface $F(u, v) = 0$, each point of which parametrises a different B-brane $\mathcal{C}$.

Thus, comparing the A- and B-models:

$$\partial_v W_B = u = \cdots \{F(u, v) = 0\} \cdots \stackrel{!}{=} \partial_v \left(\sum_{n\geq 1} \sum_{k,m} \frac{d_{k,m}}{n^2} (\mathrm{e}^{-t})^{nk} (\mathrm{e}^{v})^{nm} \right) = \partial_v W_A,$$

and the dots mean that we solve $F(u, v) = 0$ for u to obtain an expression dependent on v and—through (4)—on e^{-t}.

5. Appreciation of the AV method

The method of [1] is quite powerful, as it only requires knowledge of the mirror CY (specifically of the mirror superpotential $W(y_i)$ or $F(u, v)$) to extract A-model instanton numbers. Indeed, the result of the B-model Chern–Simons action ($\partial_v W_B = u$) is independent of the mirror CY or the mirror B-brane.

The drawback is that it is not clear how the instanton numbers depend on the choice of A-branes. Would different charges q^α yield different instantons numbers? In their examples, the choices of q^α yield convenient A- and B-branes. Maybe a different choice would not allow for several phases in which the brane splits, or would not allow us to identify one of the variables u, v with the size of disk instantons. It seems that given a mirror CY (or even the A-model CY for that matter), there is a unique choice of A-brane for which we can compute A-model instantons.

Another constraint of the method is that it only works for $k = 3$, as it relies on the Chern–Simons theory for the B-model topological string, which presupposes three-folds as target spaces.

6. Example: the resolved conifold

We now turn to a non-compact example of CY_3, namely the resolved conifold: $\mathcal{O}(-1) \times \mathcal{O}(-1) \to \mathbf{P}^1$, a rank two concave bundle over the complex line. H_2 of the CY_3 is thus $H_2(\mathbf{P}^1) = \mathbb{Z}$, while the A-brane is a Lagrangian submanifold cutting the base $\mathbf{P}^1$ in a circle S^1, and $H_1(S^1) = \mathbb{Z}$. Thus both k and m are merely integers and t, v merely complex numbers. The input from the B-model is an explicit expression for the derivative of the superpotential [1]:

$$\begin{aligned}\partial_v W &= \log\left(\frac{1-\mathrm{e}^v}{2} + \frac{1}{2}\sqrt{(1-\mathrm{e}^v)^2 + 4\mathrm{e}^{-t+v}}\right) = \log\left(\frac{1-y}{2} + \frac{1}{2}\sqrt{(1-y)^2 + 4qy}\right)\\ &= \sum_{k\geq 0, m\geq k} \frac{(-1)^{k+1}}{m+k}\binom{m+k}{k}\binom{m}{k} q^k y^m\\ &:= \sum_{k\geq 0, m\geq k} C_{k,m} q^k y^m \quad \text{with}\, C_{0,0} = 0,\end{aligned} \tag{8}$$

where v is the (rescaled) natural variable in the phase where the mirror B-brane degenerates to two submanifolds passing through the south pole of the resolved conifold. This v also measures the size of the minimal holomorphic disk passing through the south pole and ending on the Lagrangian submanifold. Precisely when the submanifold splits into several components can we wrap the A-brane around any of those, and guarantee that it will not deform (as it would otherwise acquire a boundary). This phase is characterised by $\mathrm{e}^v \to 0$, agreeing with the large volume limit on the A-model side.

To detail how we arrived at the Taylor expansion of (8) in the large volume limit $\mathrm{e}^v \to 0$, it is best to differentiate both sides w.r.t. q and set $a := 1 + 4qy/(1-y)^2$:

$$\begin{aligned}\frac{2y}{(1-y)^2}\frac{1}{a+\sqrt{a}} &= \frac{2y}{(1-y)^2}\left(\frac{1}{\sqrt{a}} - 1\right)\frac{1}{1-a} = \frac{-1}{2q}\left(\frac{1}{\sqrt{a}} - 1\right)\\ &= \frac{-1}{2q}\sum_{k\geq 1}\binom{-\frac{1}{2}}{k}\left(\frac{4qy}{(1-y)^2}\right)^k\\ &= \frac{-1}{2q}\sum_{k\geq 1} q^k(-1)^k 2\binom{2k-1}{k}\sum_{i\geq 0}\binom{2k+i-1}{i} y^{i+k}\\ &= \sum_{k\geq 0, m\geq k} q^k y^m (-1)^k \binom{2k+1}{k}\binom{m+k}{2k+1}\\ &= \sum_{k\geq 0, m\geq k} q^k y^m (-1)^k \binom{m}{k+1}\binom{m+k}{k}.\end{aligned}$$

And this agrees with the above:

$$C_{k,m} = \frac{(-1)^{k+1}}{k}\binom{m+k-1}{k-1}\binom{m}{k} = \frac{(-1)^{k+1}}{m+k}\binom{m+k}{k}\binom{m}{k}. \tag{9}$$

As far as the constant of integration is concerned (the q^0 term of (8)), note that $\sum_{m\geq 0} C_{0,m} y^m = \sum_{m\geq 1} -y^m/m = \log(1-y)$, in agreement with the first expression of (8) which goes like $\log(1-y+\mathrm{O}(q)) = \log(1-y)+\mathrm{O}(q)$.

Comparing this to the A-model expression (1)

$$\partial_v W = -\sum_{k,m} m d_{k,m} \log(1-q^k y^m) = \sum_{k,m} \left(\sum_{l|(k,m)} d_{k/l,m/l} \frac{m}{l^2} \right) q^k y^m,$$

we can recursively extract the values of all $d_{k,m}$ from the relation

$$C_{k,m} = \sum_{l|(k,m)} d_{k/l,m/l} \frac{m}{l^2}. \tag{10}$$

Proposition 1. *With the $C_{k,m}$ as in (9), the instanton numbers $d_{k,m}$ are all integers.*

Proof. We proceed step by step, according to the greatest common divisor (gcd) of k and m:

- $(k,m)=1$: From (10) we have $C_{k,m} = d_{k,m} m$. So for $d_{k,m}$ to be integer, we need $C_{k,m}$ to be $0 \bmod m$. Note that in general, $(n,k)=1$ implies

  $$n \left| \binom{n}{k} \right.,$$

  since

  $$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}.$$

  Thus $C_{k,m} \in \mathbb{Z}$ and even $\in m\mathbb{Z}$.
- $(k,m)=p^l$: For p prime. This time

  $$C_{k,m} = d_{k,m} m + d_{k/p,m/p}\frac{m}{p^2} + \cdots + d_{k/p^l,m/p^l}\frac{m}{p^{2l}} = d_{k,m} m + \frac{1}{p} C_{k/p,m/p}.$$

  Thus for $d_{k,m}$ to be integer, we need $C_{k,m} \equiv (1/p)C_{k/p,m/p} \bmod m$, i.e. $pC_{p^l k, p^l m} \equiv C_{p^{l-1}k, p^{l-1}m} \bmod mp^{l+1}$ for $(k,m)=1$, i.e.

  $$\binom{p^l(m+k)}{p^l k}\binom{p^l m}{p^l k} - \binom{p^{l-1}(m+k)}{p^{l-1}k}\binom{p^{l-1}m}{p^{l-1}k} \equiv 0 \bmod mp^{2l}.$$

  Lemma A.1 tells us that the congruence is valid mod p^{3l} $(p>3)$ or mod p^{3l-1} $(\forall\, p)$, hence also mod p^{2l} for any prime p. Since

  $$m \left| \binom{p^l m}{p^l k} \right.,$$

  both terms also contain a factor of m, and the congruence is valid mod mp^{2l}.

- $(k, m) = pq$: For primes p and q. Again by (10) we have

$$C_{k,m} = d_{k,m}m + d_{k/p,m/p}\frac{m}{p^2} + d_{k/q,m/q}\frac{m}{q^2} + d_{k/pq,m/pq}\frac{m}{p^2q^2}$$
$$= d_{k,m}m + \frac{1}{p}C_{k/p,m/p} + \frac{1}{q}C_{k/q,m/q} - \frac{1}{pq}C_{k/pq,m/pq}.$$

Thus we need $pqC_{pqk,pqm} - qC_{qk,qm} - pC_{pk,pm} + C_{k,m} \equiv 0 \bmod mp^2q^2$ for $(k, m) = 1$, i.e.

$$\binom{pq(m+k)}{pqk}\binom{pqm}{pqk} - \binom{q(m+k)}{qk}\binom{qm}{qk} - \binom{p(m+k)}{pk}\binom{pm}{pk}$$
$$+\binom{m+k}{k}\binom{m}{k} \equiv 0 \bmod mq^2p^2.$$

Again by Lemma A.1, the first difference is $0 \bmod p^3$ ($p > 3$, or mod p^2 $\forall$ p), so is the last difference, and we can factor out p^2, hence also q^2. As before, we can also take out a factor of m, and the whole line is thus $0 \bmod mp^2q^2$.

- $(k, m) = pqr$: For primes p, q and r. As before, the principle of inclusion and exclusion yields the requirement

$$pqrC_{pqrk,pqrm} - qrC_{qrk,qrm} - prC_{prk,prm} - pqC_{pqk,pqm} + rC_{rk,rm} + qC_{qk,qm}$$
$$+ pC_{pk,pm} - C_{k,m} \equiv 0 \bmod mp^2q^2r^2$$

for $(m, k) = 1$. Reasoning as above and noting that the four pairs $(pqrC_{pqrk,pqrm} - qrC_{qrk,qrm})$, $(prC_{prk,prm} - rC_{rk,rm})$, $(pqC_{pqk,pqm} - qC_{qk,qm})$ and $(pC_{pk,pm} - C_{k,m})$ are all $0 \bmod p^2$, we find that the requirement is met.

- $(k, m) = p^lq$: For p, q prime. Now we have

$$C_{k,m} = d_{k,m}m + \frac{1}{p}C_{k/p,m/p} + \frac{1}{q}C_{k/q,m/q} - \frac{1}{pq}C_{k/pq,m/pq},$$

so we are back at a combination of the cases $(k, m) = p^l$ and $(k, m) = pq$, and the same reasoning will show that $d_{k,m}$ is again integer. □

Having covered the cases of (k, m) being product of primes and powers of primes, inductive reasoning will show that the same conclusion will be met in the most general case where $(k, m) = p_1^{l_1} \dots p_j^{l_j}$.

7. Example: degenerate $\mathbf{P}^1 \times \mathbf{P}^1$

Our second example of non-compact CY_3 is a concave line bundle over two complex lines: $\mathcal{O}(-3) \to \mathbf{P}^1 \times \mathbf{P}^1$, with Kähler moduli t_1, t_2 describing the sizes of the two complex lines (or real spheres). An easy mirror map is only known for the degenerate case where the size of the second $\mathbf{P}^1$ goes to infinity; that is we retain only one modulus, t_1, with associated variable $q = \mathrm{e}^{-t_1}$. And so—as in the previous example—k and m are both integers.

This time the input from the B-model is [1]:

$$\partial_v W = \log\left(\frac{1+q-y}{2} + \frac{1}{2}\sqrt{(1+q-y)^2 - 4q}\right) = \sum_{k\geq 0, m\geq 1} \frac{-1}{m}\binom{m+k-1}{k}^2 q^k y^m =: \sum_{k,m\geq 0} C_{k,m} q^k y^m \quad \text{with } C_{k,0} = 0, \quad (11)$$

where v is the (rescaled) natural variable in the phase where the projection of the A-brane on the base is a circle on the $\mathbf{P}^1$ of infinite volume. In order to understand the double series expansion, we proceed as in the previous example, but now we differentiate both sides w.r.t. y and obtain—up to a minus sign—something symmetric in q and y:

$$\begin{aligned}
&\frac{1}{\sqrt{(1+q-y)^2 - 4q}} \\
&= \frac{1}{\sqrt{(1-q-y)^2 - 4qy}} = \frac{1}{1+q-y}\sum_{n\geq 0}\binom{-\frac{1}{2}}{n}\left(\frac{-4q}{(1+q-y)^2}\right)^n \\
&= \sum_{n\geq 0}\binom{-\frac{1}{2}}{n}(-4q)^n \sum_{i\geq 0}\binom{i+2n}{i}(y-q)^i \\
&= \sum_{m\geq 0} y^m \sum_{n\geq 0}\binom{-\frac{1}{2}}{n}(-4q)^n \sum_{i\geq 0}\binom{m+i+2n}{m+i}\binom{m+i}{n}(-q)^i \\
&= \sum_{m\geq 0} y^m \sum_{k\geq 0} q^k(-1)^k \sum_{n=0}^{k}\binom{-\frac{1}{2}}{n} 4^n \binom{m+k+n}{m+k-n}\binom{m+k-n}{m} \\
&= \sum_{m\geq 0} y^m \sum_{k\geq 0} q^k(-1)^k \sum_{n=0}^{k} 2(-1)^n \frac{(2n-1)!}{(n-1)!n!}\frac{(m+k+n)!}{(2n)!m!(k-n)!} \\
&= \sum_{m\geq 0} y^m \sum_{k\geq 0} q^k(-1)^k \binom{m+k}{k}\sum_{n=0}^{k}(-1)^n\binom{m+k+n}{n}\binom{k}{n} \\
&= \sum_{m\geq 0} y^m \sum_{k\geq 0} q^k \binom{m+k}{k}^2,
\end{aligned}$$

where we have used: the last sum over n is but the contribution to the power x^k in the expansion of the product of $(x-1)^k$ and $(1/1-x)^{m+k+1}$; and since this product equals $(-1)^k(1+x+x^2+\cdots)^{m+1}$, the sum equals

$$(-1)^k\binom{m+k}{k}.$$

And this agrees with the $C_{k,m}$ above:[1]

$$C_{k,m} = -\frac{1}{m}\binom{m+k-1}{k}^2 = -\frac{1}{k}\binom{m+k-1}{k}\binom{m+k-1}{k-1} = -\frac{m}{(m+k)^2}\binom{m+k}{m}^2, \tag{12}$$

of which only the last version is suitable for the case $m = 0 : C_{k,0} = 0$. The latter yields also the constant of integration (the y^0 term of (11)), since $\sum_{k\geq 0} C_{k,0}q^k = 0$, in agreement with the first expression of (8) which goes like $\log((1+q-y)/2 + (1-q)/2 + \mathrm{O}(y)) = \log(1+\mathrm{O}(y)) = \mathrm{O}(y)$.

Proposition 2. *With the $C_{k,m}$ as in (12), the instanton numbers $d_{k,m}$ are all integers.*

Proof. The logic remains the same, and we proceed again inductively on the nature of the gcd of k and m:

- $(k, m) = 1$: As before, we need $C_{k,m} \equiv 0 \bmod m$, which is readily seen from (12).
- $(k, m) = p^l$: As before, the requirement boils down to $pC_{p^l k, p^l m} \equiv C_{p^{l-1}k, p^{l-1}m} \bmod mp^l$ for $(k, m) = 1$, i.e.

$$\frac{m}{(m+k)^2}\left[\binom{p^l(m+k)}{p^l m}^2 - \binom{p^{l-1}(m+k)}{p^{l-1}m}^2\right] \equiv 0 \bmod mp^{2l},$$

  i.e.

$$\binom{p^l(m+k)}{p^l m} \equiv \pm\binom{p^{l-1}(m+k)}{p^{l-1}m} \equiv 0 \bmod p^{2l},$$

  which is again fine by Lemma A.1.
- $(k, m) = pq$: The same requirement as in (11) stipulates

$$\binom{pq(m+k)}{pqk}^2 - \binom{q(m+k)}{qk}^2 - \binom{p(m+k)}{pk}^2 + \binom{m+k}{k}^2 \equiv 0 \bmod q^2p^2$$

  for $(k, m) = 1$. Again, by Lemma A.1, the first difference is $0 \bmod p^3$, so is the second, and similarly for $\bmod q^3$.

[1] Note that in [1], the $C_{k,m}$ have the following form:

$$C_{k,m} = \frac{(-1)^{k+1}}{m+k}\binom{m+k}{k} + \sum_{n=1}^{k}\frac{(-1)^{k+n+1}}{m+k+n}\frac{(m+k+n)!}{n!n!m!(k-n)!},$$

where the first term is just the $n = 0$ term of the sum next to it and is the coefficient in the expansion of $\log(1+q-y)$, so that the expression agrees with our own one.

The cases $(k, m) = pqr$ and $(k, m) = p^l q$ can be imported without change from the previous example, and thus the integrality of the $d_{k,m}$ is proved for the most general case of $(k, m) = p_1^{l_1} \ldots p_j^{l_j}$. □

Acknowledgements

Thanks to Emanuel Scheidegger for his unremitting help, to Matthijs Coster for his contribution towards Lemma A.1, to Pieter Moree for stimulating discussion and to Robbert Dijkgraaf for the final touch.

Appendix A

We now prove a lemma from number theory, involving congruences of binomial coefficients.

Lemma A.1. *For p prime and $n, k \in \mathbb{N}$ we have*

$$\binom{np^l}{kp^l} \equiv \binom{np^{l-1}}{kp^{l-1}} \bmod p^{3l} \quad \textit{for } p > 3 \quad (\textit{and} \bmod p^{3l-1} \forall\, p).$$

Proof. We use the notation $\prod'$, $\sum'$ for a product or a sum skipping multiples of p, and we define $S(n) := \sum_{i=1}^{\prime n} 1/i$ and $S_2(n) := \sum_{i=1}^{\prime n} 1/i^2$. Note also that all non-multiples of p have an inverse, i.e. that $(\mathbb{Z}/p^l\mathbb{Z})^*$ is a multiplicative group. We have

$$\prod_{i=1}^{kp^l}{}' \left(1 + \frac{kp^l}{i}\right) = \prod{}' \frac{kp^l + i}{i} \frac{kp^l - i}{i} = \prod{}' \left(1 - \frac{k^2 p^{2l}}{i^2}\right) \equiv 1 + k^2 p^{2l} S_2(kp^l) \bmod p^{4l},$$

except for an extra minus sign for the second line if $p = 2$, $l = 1$, k odd. The LHS is $1 + S(kp^l)kp^l - ((S^2(kp^l) - S_2(kp^l))/2)k^2 p^{2l} \bmod p^{3l}$. Comparing both sides $\bmod p^{2l}$, we find that $S(kp^l) \equiv 0 \bmod p^l$. Comparing $\bmod p^{3l}$ yields $kS(kp^l) + (k^2/2)S_2 (kp^l)p^l \equiv 0 \bmod p^{2l}$; and using $S_2(kp^l) \equiv 0 \bmod p^l$ $(p > 3)$ from Lemma A.2, we obtain

$$S(kp^l) \equiv 0 \bmod p^{2l} \quad \text{for } p > 3,$$

while only $\bmod p^{2l-1}$ for $p = 3$, and $\bmod p^{2l-2}$ for $p = 2$ (as the coefficient 1/2 takes away one power of p).

We now turn to the binomial coefficients: note first that they both have the same number of multiples of p, namely the number of multiples of p lying in the interval $[n - k, n]$ or $[k, n]$—whichever interval is smaller. We assume that they actually do not contain multiples of p, so that we can consider their quotient. If they do, their difference will contain even more powers of p than p^{3l}, so that we could strengthen our result

$$\frac{\binom{np^l}{kp^l}}{\binom{np^{l-1}}{kp^{l-1}}} = \frac{np^l \dots ((n-k)p^l+1)}{np^{l-1}\cdots((n-k)p^{l-1}+1)} \frac{(kp^{l-1})!}{(kp^l)!}$$

$$= \prod_{i=1}^{kp^l}{}' \frac{(n-k)p^l+i}{p^{-kp^{l-1}}} \frac{p^{-kp^{l-1}}}{kp^l-i} = \prod{}' \frac{(n-k)p^l+i}{i} = \prod{}' \left(1+\frac{(n-k)p^l}{i}\right)$$

$$\equiv 1+p^l(n-k)S(kp^l)+p^{2l}(n-k)^2\frac{S^2(kp^l)-S_2(kp^l)}{2} \bmod p^{3l}$$

$$\equiv 1 \bmod p^{3l}$$

by the above. □

As a special case of the lemma, for $n = 2$, $k, l = 1$, we obtain

$$\binom{2p}{p} \equiv 2 \bmod p^3,$$

or Wolstenholme's theorem.

Corollary A.1.

$$\binom{2p-1}{p-1} \equiv 1 \bmod p^3 \quad \textit{for } p > 3 \quad (\textit{and} \bmod p^2\ \forall\, p).$$

Lemma A.2. *For $l, n \in \mathbb{N}$ and p prime we have*

$$S_n(p^l) := \sum_{i=1}^{p^l}{}' \frac{1}{i^n} \equiv 0 \equiv \sum_{i=1}^{p^l}{}' i^n \bmod p^l \quad \textit{if}\ (p-1) \nmid n,$$

and $0 \bmod p^{l-1}$ *for any* p, n.

Proof. Note that the same is true of $S_n(kp^l)$ for $k \in \mathbb{N}$, as this is merely k copies (mod p^l) of $S_n(p^l)$. Similarly, $S_n(p^{l+1})$ is just p equal copies (mod p^l) of $S_n(p^l)$, so by induction, we only need to prove the result for $S_n(p)$.

Let ζ be a primitive root mod p, i.e. a number such that the set $\{1, \zeta, \zeta^2, \dots, \zeta^{\phi-1}\}$ covers all elements of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ of order $\phi(p) = p - 1$. That is, the set is equal (mod p) to $\{1, 2, \dots, p-1\}$; and similarly the set $\{1, 1/2^n, \dots, 1/(p-1)^n\}'$ is equal (mod p^l) to $\{1, \zeta^n, \zeta^{2n}, \dots, \zeta^{n(p-2)}\}$. Hence

$$S_n(p) \equiv 1 + \zeta^n + \cdots + \zeta^{n(p-2)} = \frac{1-\zeta^{n(p-1)}}{1-\zeta^n} \equiv 0 \bmod p,$$

since $\zeta^{p-1} \equiv 1 \bmod p$. For the denominator $1 - \zeta^n$ to be invertible mod p, we must exclude the case where $\zeta^n \equiv 1 \bmod p$, i.e. where n is a multiple of $p - 1$. In this case, it still is true that $S_n(p) \equiv 0 \bmod p^0$, i.e. $0 \bmod 1$.

For $\sum' i^n$, the proof runs similarly. Note that in this case we could drop the dash from the sum to include multiples of p, as their contribution would be $p(1 + 2 + \cdots + p^{l-1}) = p^l(p^{l-1} + 1)/2$. □

One could have tackled the proof of Lemma A.1 in other ways, in particular by writing out the binomial coefficients as factorials and using properties of factorials. For the sake of completeness, we include a useful property of residues of factorials (Wilson's theorem).

Proposition A.1. *For p prime we have*

$$(p - 1)! \equiv -1 \bmod p \quad (p > 2),$$

and $1 \bmod p$ *for* $p = 2$.

Proof. In the product $1 \ldots (p-1)$, the numbers occur in pairs j and $1/j \bmod p$, except for 1 and $p-1$ which are their own inverses, since these are the only solutions of $j^2-1 \equiv 0 \bmod p$. Thus the product is $1(p - 1) \equiv -1 \bmod p$. For $p = 2$, 1 and $p - 1$ are equal mod p. □

For higher powers of the prime p, $p^k!$ contains a factor of $p^{1+p+p^2+\cdots+p^{k-1}}$. We introduce the dash notation to indicate that we have skipped all these multiples of p: $p^k!' = p^k!/(p^{k-1}!(p)^{p^{k-1}})$. We compute the residue mod p: $(p^k - 1)!' = (1 \ldots p^{k-1} \ldots 2p^{k-1} \ldots pp^{k-1})'$ consists of p times $(p^{k-1} - 1)!' \bmod p$. By induction, this yields the following lemma.

Lemma A.3. *For p prime and $k \in \mathbb{N}$ we have*

$$(p^k - 1)!' \equiv -1 \bmod p \quad (p > 2),$$

and $1 \bmod p$ *for* $p = 2$.

More generally, this result holds also mod p^l for powers $k \geq l$, as we shall show below.

Lemma A.4. *For p prime we have*:

$$(p^{k-1} - 1)!' \equiv (p - 1)!^{p^{k-2}} \equiv -1 + n_1 p^{k-1} \bmod p^k \quad (p > 2, k \geq 2),$$

and $\equiv 1 + p^{kl-1} \bmod p^k$ *for* $p = 2, k \geq 4$.

Here, $n_1 \in \mathbb{Z}_p$ *is defined by* $(p - 1)! \equiv -1 + n_1 p \bmod p^2 (p > 2)$.

Proof. By induction on k. The case $k = 2$ is trivial

$$(p^{k-1} - 1)!' = [1 \cdot 2 \ldots (p^{k-2} - 1)]'[(p^{k-2} + 1) \cdots (p^{k-2} + p^{k-2} - 1)]' \cdots [((p - 1)p^{k-2} + 1) \cdots (p^{k-1} - 1)]'.$$

The first square bracket is $-1 + n_1 p^{k-2} \bmod p^{k-1}$ by induction, i.e. it is $-1 + n_1 p^{k-2} + cp^{k-1} \bmod p^k$ (for some integer c), a quantity we denote by a. The second square bracket is $a + p^{k-2}(p^{k-2} - 1)!' S_1(p^{k-2}) \bmod p^k$. Since $S_1(p^{k-2}) \equiv 0 \bmod p^{k-2}$ by Lemma A.2 ($p \neq 2$), this is just $a \bmod p^k$ if $k > 3$. (For $k = 3$, a trailing $p^2 \cdot$ const would not affect the ultimate conclusion.) All remaining brackets are also $a \bmod p^k$. Hence

$$(p^{k-1} - 1)!' \equiv a^p \equiv (-1 + n_1 p^{k-2})^p \equiv -1 + n_1 p^{k-1} \equiv (-1 + n_1 p)^{p^{k-2}} \bmod p^k.$$

For $p = 2$, the anchor is at $k = 4 : (p^3 - 1)!' = 1\,3\,5\,7 \equiv 1 + 2^3 \bmod p^4$. So the last line reads $a^p \equiv 1 + p^{k-1} \bmod p^k$. Since we only have $S_1(p^{k-2}) \equiv 0 \bmod p^{k-3}$, there is a trailing p^{2k-5}, which is fine for the induction with $k \geq 5$. □

Corollary A.2.

$$(p^k - 1)!' \equiv -1 \bmod p^k \quad (p > 2),$$

and $1 \bmod p^k$ *for* $p = 2$.

Proof. LHS $= [1 \ldots (p^{k-1} - 1)]'[(p^{k-1} + 1) \ldots (p^{k-1} + p^{k-1} - 1)]' \cdots [((p-1)p^{k-1} + 1) \cdots (p^k - 1)]'$. By the previous lemma, the first square bracket yields $(p-1)!^{p^{k-2}}$ $(p > 2)$, while the second yields the same plus $p^{k-1}(p-1)!S_1(p)$ (which is $0 \bmod p^k$), and all other square brackets yield the same. In all we have $(p-1)!^{p^{k-1}} \equiv (-1 + n_1 p + \cdots)^{p^{k-1}} \equiv -1 \bmod p^k$ (or $+1$ for $p = 2$). □

The same method of proof easily yields the following proposition.

Proposition A.2. *For prime* p *and integers* $k \geq l$ *we have*

$$(p^k - 1)!' \equiv -1 \bmod p^l \quad (p > 2),$$

and $1 \bmod p^l$ *for* $p = 2$.

There is no explicit formula for $(p - 1)! \bmod p^2$, i.e. the integer n_1 in $(p - 1)! \equiv -1 + n_1 p \bmod p^2$ is no evident function of p. In Hardy and Wright, one will find a formula reducing the factorial to terms involving $p - 1/2!$. Also, for mod p^3, the recent literature exhibits ways to reduce the factorial to complicated terms involving the class number of p.

References

[1] M. Aganagic, C. Vafa, Mirror Symmetry, D-Branes and Counting Holomorphic Discs. hep-th/0012041.

[2] H. Ooguri, C. Vafa, Knot invariants and topological strings, Nucl. Phys. B 577 (2000) 419–438. hep-th/9912123.