Sequences of enumerative geometry: congruences and asymptotics

Daniel B. Grünberg, Pieter Moree

Appendix by Don Zagier

Abstract

We study the integer sequence v_n of numbers of lines in hypersurfaces of degree $2n-3$ of $\mathbb{P}^n$, $n > 1$. We prove a number of congruence properties of these numbers of several different types. Furthermore, the asymptotics of the v_n are described (in an appendix by Don Zagier). An attempt is made at a similar analysis of two other enumerative sequences: the numbers of rational plane curves and the numbers of instantons in the quintic threefold.

We study the sequence of numbers of lines in a hypersurface of degree $D = 2n - 3$ of $\mathbb{P}^n$, $n > 1$. The sequence is defined by (see e.g. [8])

$$v_n := \int_{G(2,n+1)} c_{2n-2}(\mathrm{Sym}^D Q), \tag{1}$$

where $G(2, n+1)$ is the Grassmannian of $\mathbb{C}^2$ subspaces of $\mathbb{C}^{n+1}$ (i.e. projective lines in $\mathbb{P}^n$) of dimension $2(n+1-2) = 2n-2$, Q is the bundle of linear forms on the line (of rank $r = 2$, corresponding to a particular point of the Grassmannian), and Sym^D is its Dth symmetric product – of rank $\binom{D+r-1}{r-1} = D-1 = 2n-2$. The top Chern class (Euler class) c_{2n-2} is the class dual to the 0-chain (i.e. points) corresponding to the zeros of the bundle $\mathrm{Sym}^D(Q)$, i.e. to the vanishing of a degree D equation in $\mathbb{P}^n$; this is the geometric requirement that the lines lie in a hypersurface.

The integral (1) can actually be written as a sum:

$$v_n = \sum_{0 \le i < j \le n} \frac{\prod_{a=0}^{D}(aw_i + (D-a)w_j)}{\prod_{0 \le k \le n,\ k \ne i,j}(w_i - w_k)(w_j - w_k)}, \tag{2}$$

where $w_0, \ldots, w_n$ are arbitrary complex variables. This is a consequence of a localisation formula due to Atiyah and Bott from equivariant cohomology, which says that only the (isolated) fixed points of the $(\mathbb{C}^*)^{n+1}$ action contribute to the defining integral of v_n. Hence the sum. For the first few values of n computation yields $v_2 = 1$, $v_3 = 27$, $v_4 = 2875$, $v_5 = 698005$, $v_6 = 305093061$.

D. Zagier gave a simple proof that the right hand side of (2) is independent of

Mathematics Subject Classification (2000). 14N10, 11A07, 41A60

$w_0, \ldots, w_n$ (as it must be for (2) to hold), and that in fact it can be replaced by the much simpler formula

$$v_n = \left[(1-x)\prod_{j=0}^{2n-3}(2n-3-j+jx)\right]_{x^{n-1}} \tag{3}$$

where the notation $[\ldots]_{x^n}$ means the coefficient of x^n. In fact, formula (2) was proved in a very different way using methods from Schubert calculus by B.L. van der Waerden, who established it in part 2 of his celebrated 20 part 'Zur algebraischen Geometrie' series of papers [19, 20]. The number of linear subspaces of dimension k contained in a generic hypersurface of degree d in $\mathbb{P}^n$, when it is finite, can be likewise expressed as the coefficient of a monomial in a certain polynomial in several variables, see e.g. [15, Theorem 3.5.18].

Zagier also gave the formula

$$v_n \sim \sqrt{\frac{27}{\pi}}(2n-3)^{2n-7/2}\left(1-\frac{9}{8n}-\frac{111}{640n^2}-\frac{9999}{25600n^3}+\cdots\right), \tag{4}$$

where the right hand side is an asymptotic expansion in powers of n^{-1} with rational coefficients that can be explicitly computed. The proof of this formula, as well as the derivation of (3) from (2), can be found in the appendix.

The remaining results, summarized in Theorem 1 and Theorem 2, are concerned with congruence properties of the numbers v_n. In this context it turns out to be convenient to define $v_1 = 1$ (even though there is no such thing as a hypersurface in $\mathbb{P}^1$ of degree -1) and even more remarkably $v_0 = -1$. We do not doubt that the congruence results presented here form only the tip of an iceberg.

A first version of this paper was single authored by the first author. Indeed, the present version of this paper is similar to the first one, except for sections 2 and 3 which have been greatly revised and expanded by the second author. The conjectures outside these two sections are due to the first author alone. Sections 4 and 5 were revised by both the second author and Don Zagier.

1 Introduction

The motivating idea behind this paper is the expectation that certain problems in enumerative geometry are coupled to modularity. This is a recurrent theme in string theory, where partition functions have often an enumerative interpretation as counting objects (instantons, etc) and must satisfy the condition of modularity covariance in order to obtain the same amplitude when two worldsheets have the same intrinsic geometry.

Modular forms, as is well known, have Fourier coefficients satisfying many interesting congruences (think of Ramanujan's congruences for partitions, or for his function $\tau(n)$). The same can happen for the coefficients of expansions related to modular forms, e.g. the expansions $y = \sum A_n x^n$ obtained by writing a modular form y (locally) as a power series in a modular function x. For instance, the famous Apéry numbers related to Apéry's proof of the irrationality of $\zeta(3)$ are obtainable in this way [3] and satisfy many interesting congruences [18]. The numbers appearing in the context of mirror symmetry, Picard-Fuchs equations for Calabi-Yau manifolds, Gromov-Witten invariants and similar problems of enumerative geometry are sometimes related to modular forms and sometimes not, so we can reasonably hope for interesting congruence properties in these contexts also. In Section 2 we shall find astonishingly many congruences for our sequence v_n. We shall first draw a few tables for congruences mod 2,3,4,5 or 11, and then summarize the observed congruences. In Section 3 we prove those congruences by elementary means starting from (3), and a few conjectures will be formulated. Sequences of numbers coming from modular forms also often have interesting asymptotic properties and we therefore wish to study this, too. In Section 4 we find the asymptotic properties of the v_n numerically by using a clever empirical trick shown to us by Don Zagier which we call the asymp$_k$ trick. (A rigorous proof of these asymptotics, as already mentioned above, was also provided by him and is reproduced in the appendix.) Section 5 presents congruences and asymptotics for two further examples of enumerative sequences, without proofs. The sequence of rational curves on the plane and the sequence of instantons on the quintic threefolds partly partly mimic the behaviour of the original sequence of lines in hypersurfaces.

2 Congruences

We will consider the sequences $\{v_n \pmod{k}\}_{k=1}^{\infty}$ for some small values of k; that is, we study the reduction of the integers v_n modulo k. It turns out to be instructive to order the v_n modulo k in a table. Each table has k columns. The ith column ($i = 1, \dots, k$) gives the values of $v_{lk+i} \pmod{k}$ ($l \geq 0$).

For instance, the first few tables at $k = 2, 3, 4, \dots$ look like

$\underline{k=2}$:

1	1	1	1	1	1	1	...
1	1	1	1	1	1	1	...

$\underline{k=3}$:

1	1	2	2	2	0	0	0	2	...
1	1	2	2	2	0	0	0	2	...
0	0	0	0	0	0	0	0	0	...

$\underline{k=4}$:

1	1	1	1	1	1	1	...
1	1	1	1	1	1	1	...
3	3	3	3	3	3	3	...
3	3	3	3	3	3	3	...

$\underline{k=5}$:

1	1	4	4	4	4	4	2	3	...
1	1	4	4	4	4	4	2	3	...
2	0	0	2	3	2	1	4	1	...
0	0	0	0	0	0	0	0	0	...
0	1	0	0	0	0	4	0	0	...

The first table ($k = 2$) says that all the v_n are odd integers. We shall mostly be interested in the tables for prime k. Here is a typical prime table:

$\underline{k=11}$:

1	1	10	10	10	10	10	10	10	10	10	10	10	8	...
1	1	10	10	10	10	10	10	10	10	10	10	10	8	...
5	9	10	7	8	6	10	2	7	8	6	10	8	5	...
4	1	5	8	6	7	10	8	2	6	7	10	8	8	...
0	9	3	2	2	0	0	0	0	0	0	0	1	5	...
9	3	10	0	1	4	8	10	7	6	2	8	10	7	...
0	0	0	0	0	0	0	0	0	0	0	0	0	0	...
0	2	5	1	1	0	0	0	0	0	0	0	8	10	...
0	2	2	2	7	0	0	0	0	0	0	0	10	1	...
0	10	0	10	2	0	0	0	0	0	0	0	8	3	...
0	2	8	9	3	0	0	0	0	0	0	0	7	5	...

Study of these and other tables led us to formulate a number of conjectures, most of which we were able to prove. An overview of these results is given in Theorem 1.

Theorem 1 *The following holds for the tables of v_n mod k:*
1. *All v_n are odd.*
2. *The first two rows of each table are equal.*
3. *If k is even, then rows $k/2+1$ and $k/2+2$ are equal.*
4. *For k odd, row $(k+3)/2$ contains only zeros.*
5. *For k prime, the first two rows start with 1,1 followed by k occurrences of $k-1$.*
6. *For $k>2$ prime, the last $(k-1)/2$ slots of the first column vanish.*
7. *For $k>2$ prime, there is a block of zeros at the bottom (after $(k-1)/2$ columns), of height $(k-1)/2$ and width $(k+3)/2$.*
8. *For $k=2^q$, all rows are constant and in two fold way sweep out all odd residues, i.e. for every odd integer a with $1 \le a \le 2^q$ there are precisly two rows that have only a as entry.*
9. *For $k=2^q>2$ the entries in the rows $1,2,2^{q-1},2^{q-1}+1,2^{q-1}+2,2^q-1$ equal, respectively, $1,1,2^{q-1}-1,2^{q-1}+1,2^{q-1}+1,2^q-1$.*
10. *For $k=2^q>2$ the entries in row a and row $a+2^{q-1}$ differ by $2^{q-1} \pmod{2^q}$.*

Proof. These ten claims are proved in, respectively, lemmas 6, 3, 3, 4, 7 & 8, 11, 13, 20 & 23, 22 and 22. □

On computing the reductions of $v_1,\ldots,v_{32}$ modulo 32 one finds by part 8 of this theorem that for $k=4$ the table has constant rows $1,1,3,3$, for $k=8$ constant rows $1,1,3,3,5,5,7,7$, for $k=16$ constant rows $1,1,11,11,5,5,7,7,9,9,3,3,13,13,15,15$ and for $k=32$ constant rows $1,1,27,27,21,5,7,23,9,9,19,19,29,13,31,15,17,17,11,11,5,21,23,7,25,25,3,3,13,29,15,31$. Thus, for modulus 2^q with $q\le 3$ we observe that pairs of values occur and that these, moreover, are in ascending order. For $q=4$ the values still come in pairs, but the order is no longer ascending. For $n\ge 5$ it turns out that pairs with equal values become sparser and sparser. Notice that in the above cases for every modulus all odd values are assumed exactly twice. By part 8 this always happens. Thus, given an odd integer a and any integer $q\ge 1$ there are infinitely many integers m such that $v_m \equiv a \pmod{2^q}$ (or put more succinctly: modulo powers of two the sequence v_n is equidistributed over the odd residue classes).

For k prime, often $v_n \equiv 0 \pmod{k}$ for trivial reasons. It then makes sense to consider divisibility of v_n by higher powers of k. Our deepest result in this direction is provided by the following theorem.

Theorem 2 1. *If $p\ge 5$ is a prime, then*

$$v_{\frac{p+3}{2}} \equiv -2p^3 \pmod{p^4} \text{ and } v_{\frac{p+3}{2}} \equiv 2p^3(1-p)(p-1)!4^{p-1} \pmod{p^5}.$$

2. *Let $r\ge 1$ and $p\ge 2r+1$ be a prime. Then*

$$v_{\frac{p+3}{2}+rp} \equiv C_r p^{2r+2} \pmod{p^{2r+3}}, \tag{5}$$

where

$$C_r = \frac{r}{(-4)^{r-1}} \left(\frac{2r+1}{r!}\right)^2 \sum_{j=0}^{2r} b_{j,r}((1-2j))_{2r-1},$$

the integers $b_{j,r}$ are defined implicitly by $\prod_{a=1}^{2r}(2r+1-a+ax) = \sum_{j=0}^{2r} b_{j,r}x^j$, and $((u))_a := \prod_{j=1}^{a}(u+2j-2)$.

`Remark`. Note that $b_{2r-j,r} = b_{j,r}$. Numerical experimentation suggests that the numerator of c_r always equals a power of 2 and that the congruence (5) holds for all odd primes.

Below we record some values of c_r.

	1	2	3	4	5
c_r:	-81	$\frac{103125}{8}$	$-\frac{210171535}{64}$	$\frac{1308348857025}{1024}$	$-\frac{11660783598520749}{16384}$

3 Proofs of the theorems

3.1 Some generalities

First recall from the elementary theory of finite fields of order p, that

$$x^{p-1} - 1 \equiv \prod_{j=1}^{p-1} (x - j) \pmod{p}.$$

(Here and below the letter x denotes a variable.) By substituting $x = 0$ one obtains *Wilson's theorem*:

$$(p - 1)! \equiv -1 \pmod{p}.$$

We also recall the freshman's identity $(a + b)^p \equiv a^p + b^p \pmod{p}$, from which we infer that if $f(x) \in \mathbb{Z}[x]$, then $f(x)^p \equiv f(x^p) \pmod{p}$. These results will be freely used in the sequel, without further referring to them.

Lemma 1 *We have* $v_n \equiv 0 \pmod{(2n-3)^2}$.

Proof. The term with $j = 0$ in (3) equals $2n - 3$. The term with $j = 2n - 3$ equals $(2n-3)x$. Hence $v_n = (2n-3)^2 w_n$, where $w_n = \left[(1-x)\prod_{j=1}^{2n-4}(2n-3-j+jx)\right]_{x^{n-2}}$. $\square$

The following result was first noticed by D. Kerner. An alternative, slightly longer, proof was given by M. Vlasenko.

Lemma 2 *We have* $v_n \equiv 0 \pmod{(2n-3)^3}$.

Proof. It suffices to show that $w_n \equiv 0 \pmod{2n-3}$. Note that, modulo $2n-3$, we have that

$$\begin{aligned} w_n &\equiv \left[(1-x)\prod_{j=1}^{2n-4}(-j+jx)\right]_{x^{n-2}} \equiv -(2n-4)!\left[(x-1)^{2n-3}\right]_{x^{n-2}} \\ &= -(2n-4)!\binom{2n-3}{n-2} = -(2n-4)!\frac{2n-3}{n-1}\binom{2n-4}{n-2} = -(2n-3)!C_{n-2}, \end{aligned}$$

where $C_m := \frac{1}{m+1}\binom{2m}{m}$ is the mth *Catalan number*. The Catalan numbers are *integers* that arise in numerous counting problems. $\square$

`Remark`. It might be interesting to see whether the integers $v_n/(2n-3)^i$ with $i = 1, 2$ or 3 also have a geometric meaning.

The next result was obtained in collaboration with Alexander Blessing. It establisheds parts 2 and 3 of Theorem 1.

Lemma 3 *For $l \geq 0$ we have $v_{ln+1} \equiv v_{ln+2} \pmod{2n}$.*

Proof. Since $v_1 = v_2 = 1$ the result is trivially true for $l = 0$ and thus we may assume $l \geq 1$. We have, modulo $2n$,

$$v_{ln+1} \equiv \left[(1-x) \prod_{j=0}^{2ln-1} (-1-j+jx)\right]_{x^{ln}}.$$

Furthermore, we have, modulo $2n$,

$$\begin{aligned}
v_{ln+2} &\equiv \left[(1-x) \prod_{j=0}^{2ln+1} (1-j+jx)\right]_{x^{ln+1}} \equiv \left[(1-x)x \prod_{j=0}^{2ln}(1-j+jx)\right]_{x^{ln+1}} \\
&\equiv \left[(1-x) \prod_{j=0}^{2ln}(1-j+jx)\right]_{x^{ln}} \equiv \left[(1-x) \prod_{j=0}^{2ln}(1-(2ln-j)+(2ln-j)x)\right]_{x^{ln}} \\
&\equiv \left[(1-x) \prod_{j=0}^{2ln}(1+j-jx)\right]_{x^{ln}} \equiv \left[(1-x) \prod_{j=0}^{2ln-1} (-1)(-1-j+jx)\right]_{x^{ln}} \\
&\equiv \left[(1-x) \prod_{j=0}^{2ln-1} (-1-j+jx)\right]_{x^{ln}} \equiv v_{ln+1} \ .
\end{aligned}$$

This concludes the proof. $\square$

The next lemma generalizes Lemma 1. It implies part 4 of Theorem 1.

Lemma 4 *If k is odd, then $v_{lk+(k+3)/2} \equiv 0 \pmod{(2l+1)^2 k^{2l+2}}$.*

Proof. We have $v_{lk+(k+3)/2} \equiv [(1-x)\prod_{j=0}^{(2l+1)k}((2l+1)k-j+jx)]_{x^{lk+(k+1)/2}}$. The terms in the product with $j = 0$ and $j = (2l+1)k$ lead to a factor of $(2l+1)^2k^2$. The remaining terms in the product that are divisible by k lead to a factor k^{2l}. $\square$

3.2 The sequence $\{v_n\}_{n=1}^{\infty}$ modulo primes

The following lemma will be repeatedly used in this section.

Lemma 5 *Let p be a prime and c an integer. Then, modulo p,*

$$\prod_{i=1}^{p-1}(ix-i+c) \equiv \begin{cases} -(x-1)^{p-1} & \text{if } p|c, \\ -(x+x^2+\ldots+x^{p-1}) = \frac{x^p-x}{1-x} & \text{otherwise.} \end{cases}$$

Proof. If $p|c$, then the result is trivial, so assume $p \nmid c$. We can write

$$\prod_{i=1}^{p-1}(ix-i+c) \equiv \prod_{i=1}^{p-1} i \prod_{i=1}^{p-1}(x-1+c/i) \equiv \frac{x^p-x}{1-x},$$

where we have used that as i runs over $1, 2, \cdots, p-1$, $-1+c/i$ runs over all residues modulo p, except for -1. $\square$

The second lemma in this section is part 1 of Theorem 1.

Lemma 6 *For $n \geq 1$ we have $v_n \equiv 1 \pmod 2$.*

Proof. Modulo 2, the $2n-2$ terms in the product in (3) are alternatingly 1 and x. It thus follows that $v_n \equiv [(1-x)x^{n-1}]_{x^{n-1}} \equiv 1 \pmod 2$. This concludes the proof. $\square$

The next lemma together with Lemma 8 establishes part 5 of Theorem 1.

Lemma 7 *Let p be a prime. Then $v_{p+1} \equiv v_{p+2} \equiv 1 \pmod p$.*

Proof. Modulo p we have $v_{p+1} \equiv [(1-x)\prod_{j=1}^{p-1}(-1-j-jx)^2]_{x^p} \equiv [(1-x)\left(\frac{x^p-x}{1-x}\right)^2]_{x^p}$, where in the derivation of the first congruence we noted that modulo p the jth term in the product (3) is equal to the $(j+p)$th and in the second we used lemma 5. Now note that

$$\left[(1-x)\left(\frac{x^p-x}{1-x}\right)^2\right]_{x^p} = \left[(1-x)\left(\frac{x}{1-x}\right)^2\right]_{x^p} = \Big[\sum_{k\geq 2} x^k\Big]_{x^p} = 1.$$

Finally, by Lemma 3, v_{p+2} satisfies the same congruence as v_{p+1} modulo p. $\square$

The proof of the next lemma involves congruences for binomial coefficients. In all cases these can be found by direct computation, but often it is more convenient to invoke a classical result of E. Lucas. Let $n \geq m$ be natural numbers and write $n = a_0 + a_1p + a_2p^2 + \cdots + a_sp^s$ and $m = b_0 + b_1p + b_2p^2 + \cdots + b_sp^s$ with $0 \leq a_i, b_i \leq p-1$. Then Lucas's theorem states that

$$\binom{n}{m} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_s}{b_s} \pmod p.$$

Recall that $\binom{a}{b} = 0$ if $b > a$. For example, by direct computation we find that

$$\binom{p^2-2}{2p-2} \equiv \left[\frac{(-2)\cdots(-2p+1)}{1\cdots(2p-2)}\right]'(1-p) \equiv -(2p-1)(p-1) \equiv -1 \pmod p$$

($[\ldots]'$ means skipping multiples of p). By Lucas's theorem we find that

$$\binom{p^2-2}{2p-2} = \binom{(p-1)p+p-2}{1\cdot p+p-2} \equiv \binom{p-1}{1}\binom{p-2}{p-2} \equiv -1 \pmod p.$$

Likewise we immediately find using Lucas' theorem that, with $r=1$ and $p>3$,

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^r}.$$

(This identity with $r=2$ was proved in 1819 by Charles Babbage. For $r=3$ it follows from Wolstenholme's theorem, see F.L. Bauer [1].)

At various points we use the easy result that $\binom{p-1}{j} \equiv (-1)^j \pmod p$. To see this observe that modulo p the entries, except the two outmost ones, in the $(p+1)$th row of Pascal's triangle are zero modulo p. Since each of these entries arises as sum of two elements above it in the pth row, the entries in the pth alternate between 1 and -1. Similarly one infers that $\binom{p-2}{j} \equiv (-1)^j(j+1) \pmod p$.

For a nice survey of arithmetic properties of binomial coefficients we refer the reader to Granville [9].

Lemma 8 *Let p be a prime and $2 \le l \le p+1$. Then $v_{lp+1} \equiv v_{lp+2} \equiv -1 \pmod p$.*

Proof. We have $v_{lp+1} \equiv \Big[(1-x)P_p^l(x)\Big]_{x^{lp}} \pmod p$, say, with $P_p^l(x) := \prod_{i=1}^{p-1}(ix-i-1)^{2l}$. As before

$$\begin{aligned}
P_p^l(x) &\equiv (x+x^2+\ldots+x^{p-1})^{2l} \equiv x^{2l}\Big[(1-x^{p-1})(1+x+x^2+\ldots)\Big]^{2l} \pmod p\\
&\equiv x^{2l}\Big[\sum_{i=0}^{2l} x^{(p-1)i} \underbrace{(-1)^i\binom{2l}{i}}_{a_{i(p-1)}} \cdot \sum_{n\ge 0} x^n \underbrace{\binom{2l+n-1}{n}}_{b_n}\Big] \pmod p\\
&\equiv x^{2l}\Big[\ldots + x^{l(p-2)-1}\sum_{i=0}^{l-1} a_{(l-1-i)(p-1)} b_{(i+1)(p-1)-l-1}\\
&\qquad + x^{l(p-2)}\sum_{i=0}^{l-1} a_{(l-1-i)(p-1)} b_{(i+1)(p-1)-l} + \ldots\Big] \pmod p,
\end{aligned}$$

where we have used that

$$\left(\sum_{k\ge 0} x^k\right)^{2l} = \sum_{n\ge 0}\binom{2l+n-1}{n} x^n.$$

Thus

$$\begin{aligned}
v_{lp+1} &\equiv \sum_{i=0}^{l-1} a_{(l-1-i)(p-1)}(b_{(i+1)(p-1)-l} - b_{(i+1)(p-1)-l-1}) \pmod p\\
&\equiv \sum_{i=0}^{l-1} a_{(l-1-i)(p-1)}\binom{(i+1)(p-1)+l-2}{2l-2} \pmod p.
\end{aligned}$$

Note that

$$a_{(l-1-i)(p-1)} = (-1)^{l-1-i}\binom{2l}{l-1-i} = \begin{cases} -2l & \text{for } i = l-2;\\ 1 & \text{for } i = l-1,\end{cases}$$

and, furthermore,

$$a_{(l-1-i)(p-1)} = \begin{cases} 0 \pmod p & \text{for } i = 0,\ldots,p-l-2;\\ -1 \pmod p & \text{for } i = p-l-1.\end{cases}$$

The remainder of the proof requires a separate discussion for $l \le (p-1)/2$, for $l = (p+1)/2$, $(p+1)/2 < l < p$, for $l = p$ and for $l = p+1$.
<u>The case $l \le (p-1)/2$</u> :
Note that

$$\begin{aligned}
\binom{(i+1)(p-1)+l-2}{2l-2} &= \frac{[(i+1)p-i-l]\cdots[(i+1)p-i+l-3]}{1\cdots(2l-2)}\\
&\equiv \begin{cases} 0 \pmod p & \text{for } i = 0,\ldots,l-3;\\ \frac{(-1)\cdots(-2l+2)}{1\cdots(2l-2)} \equiv 1 \pmod p & \text{for } i = l-2;\\ \frac{(-2)\cdots(-2l+1)}{1\cdots(2l-2)} \equiv 2l-1 \pmod p & \text{for } i = l-1.\end{cases}
\end{aligned}$$

Hence in the sum for v_{lp+1}, only the terms $i = l-2$ and $i = l-1$ contribute, that is: $v_{lp+1} = -2l \cdot 1 + 1 \cdot (2l-1) \equiv -1 \pmod p$.
The case $l = (p+1)/2$:
Here we find that

$$\binom{(i+1)(p-1)+l-2}{2l-2} \equiv \begin{cases} 1 \pmod p & \text{for } i = l-2; \\ 0 \pmod p & \text{for } 0 \leq i \leq l-1,\ i \neq l-2. \end{cases}$$

Hence in the sum for v_{lp+1}, only the term $i = l-2$ contributes and we infer that $v_{lp+1} \equiv -2l \cdot 1 \equiv -1 \pmod p$.
The case $(p+1)/2 < l < p$:
Here we compute that

$$\binom{(i+1)(p-1)+l-2}{2l-2} \equiv \begin{cases} 0 \pmod p & \text{for } i = p-l, \ldots, l-3; \\ -l \pmod p & \text{for } i = p-l-1; \\ 2-l \pmod p & \text{for } i = l-2; \\ (1-2l)(l-1) \pmod p & \text{for } i = l-1. \end{cases}$$

Hence in the sum for v_{lp+1}, only the terms $i = p-l-1$, $i = l-2$ and $i = l-1$ contribute. That is: $v_{lp+1} \equiv -1 \cdot (-l) - 2l \cdot (2-l) + 1 \cdot (1-2l)(l-1) \equiv -1 \pmod p$.
The case $l = p$:
Note that

$$a_{(p-1-i)(p-1)} = (-1)^{p-1-i} \binom{2p}{p-1-i} = \begin{cases} 0 \pmod p & \text{for } i = 0, \ldots, p-2; \\ 1 \pmod p & \text{for } i = p-1, \end{cases}$$

while for $i = p-1$, $\binom{(i+1)(p-1)+p-2}{2p-2}$ boils down to $\binom{p^2-2}{2p-2} \equiv -1 \pmod p$ (see the preamble to this lemma). Hence $v_{lp+1} \equiv -1 \pmod p$.
The case $l = p+1$:
Here we find that

$$a_{(p-i)(p-1)} = (-1)^{i+1} \binom{2p+2}{p-i} \equiv \begin{cases} -2 \pmod p & \text{for } i = 0; \\ 0 \pmod p & \text{for } i = 1, \ldots, l-4; \\ 1 \pmod p & \text{for } i = l-3; \\ -2 \pmod p & \text{for } i = l-2; \\ 1 \pmod p & \text{for } i = l-1. \end{cases}$$

and

$$\binom{(i+2)(p-1)}{2p} \equiv \begin{cases} 0 \pmod p & \text{for } i = 0; \\ 1 \pmod p & \text{for } i = l-3; \\ 1 \pmod p & \text{for } i = l-2; \\ 0 \pmod p & \text{for } i = l-1. \end{cases}$$

Hence $v_{lp+1} \equiv -2 \cdot 0 + 1 \cdot 1 - 2 \cdot 1 + 1 \cdot 0 \equiv -1 \pmod p$.

This proves that in all cases, $v_{lp+1} \equiv -1 \pmod p$. By lemma 3, the same is true for v_{lp+2}. □

The cases $l = p$ and $l = p+1$ in the latter proof can be proved more succinctly as is done in the proofs of Lemma 9, respectively Lemma 10.

Lemma 9 *Let p be a prime. Then $v_{p^2+1} \equiv v_{p^2+2} \equiv -1 \pmod p$.*

Proof. Note that, modulo p, the integer v_{p^2+1} is congruent to

$$\Big[(1-x)\prod_{j=1}^{p-1}(-1-j-jx)^{2p}\Big]_{x^{p^2}} \equiv \Big[(1-x)\prod_{j=1}^{p-1}(-1-j-jx^p)^2\Big]_{x^{p^2}} \equiv \Big[\prod_{j=1}^{p-1}(-1-j-jy)^2\Big]_{y^p}.$$

On proceding as in the previous proof we find that

$$v_{p^2+1} \equiv \Big[\Big(\frac{y^p-y}{1-y}\Big)^2\Big]_{y^p} = \Big[\Big(\frac{y}{1-y}\Big)^2\Big]_{y^p} = \Big[\sum_{k\geq 1} ky^{k+1}\Big]_{y^p} \equiv -1 \pmod{p}.$$

Finally, by Lemma 3, v_{p^2+2} satisfies the same congruence as v_{p^2+1} modulo p. □

Lemma 10 *Let p be a prime. Then $v_{p^2+p+1} \equiv v_{p^2+p+2} \equiv -1 \pmod{p}$.*

Proof. We have

$$\begin{aligned}
v_{p^2+p+1} &\equiv \Big[(1-x)(x+x^2+\cdots+x^{p-1})^{2p+2}\Big]_{x^{p^2+p}} \pmod{p}\\
&\equiv \Big[(1-x)(x+x^2+\cdots+x^{p-1})^2(x^p+\cdots+x^{p(p-1)})^2\Big]_{x^{p^2+p}} \pmod{p}\\
&\equiv \Big[(x-x^p)(x+x^2+\cdots+x^{p-1})\Big(\sum_{k=1}^{\infty}x^{kp}\Big)^2\Big]_{x^{p^2+p}} \pmod{p}\\
&\equiv \Big[(x^2+\cdots+x^p-x^{p+1}-\cdots-x^{2p-1})\sum_{k=0}^{\infty}(k+1)x^{kp}\Big]_{x^{p^2-p}}\\
&\equiv \Big[\sum_{k=0}^{\infty}(k+1)x^{(k+1)p}\Big]_{x^{p^2-p}} \equiv -1 \pmod{p}.
\end{aligned}$$

Finally, by Lemma 3, v_{p^2+p+2} satisfies the same congruence as v_{p^2+p+1} modulo p. □

The next lemma establishes part 6 of Theorem 1.

Lemma 11 *If p is an odd prime, then $v_{\frac{p+3}{2}+i} \equiv 0 \pmod{p}$ for $i = 0, \ldots, (p-3)/2$.*

Proof. In case $i=0$, the result follows by Lemma 1, so assume that $i \geq 1$. On using that modulo p the jth term equals the $(j+p)$th term, we find that, modulo p,

$$v_{\frac{p+3}{2}+i} \equiv \Big[4i^2(1-x)\prod_{j=1}^{p-1}(2i-j+jx)\prod_{j=1}^{2i}(2i-j+jx)\Big]_{x^{(p+1)/2+j}}.$$

On invoking Lemma 5 and noting that $p > \frac{p+1}{2}+i$ we infer that

$$v_{\frac{p+3}{2}+i} \equiv \Big[4i^2(x^p-x)\prod_{j=1}^{2i}(2i-j+jx)\Big]_{x^{(p+1)/2+i}} \equiv \Big[-4i^2\prod_{j=1}^{2i}(2i-j+jx)\Big]_{x^{(p-1)/2+j}}.$$

Since $\deg\Big(\prod_{j=1}^{2i}(2i-j+jx)\Big) = 2i$ and $2i < \frac{p-1}{2}+i$, the result follows. □

The next lemma will be used in the proof of Lemma 13.

Lemma 12 *Define $A_r(x)$ and $B_r(x)$ recursively by*

$$\begin{cases} A_0(x)=0,\ A_{r+1}(x)=(x+\ldots+x^{p-1})^r-A_r(x); \\ B_0(x)=0,\ B_{r+1}(x)=-(x+\ldots+x^{p-1})^r-B_r(x). \end{cases}$$

Put $f_r(x)=(x-1)(1+x^p+\ldots+x^{p(p-1)})(x+\ldots+x^{p-1})^r$. Then

$$f_r(x)=(-1)^r(x-1)(1+x^p+\ldots+x^{p(p-1)})+x^{p^2}A_r(x)+B_r(x),$$

where, for $r\ge 1$, the degree of $B_r(x)$ equals $(r-1)(p-1)$.

Proof. Easily follows on noting that

$$\begin{aligned} f_{r+1}(x) &= (1+\ldots+x^{p-1})f_r(x)-f_r(x) \\ &= (x^{p^2}-1)(x+\ldots+x^{p-1})^r-f_r(x). \end{aligned}$$

The next lemma is part 7 of Theorem 1.

Lemma 13 *Let p be an odd prime. Suppose that $0\le i\le (p-3)/2$ and $(p-1)/2\le l\le p$. Then $v_{lp+(p+3)/2+i}\equiv 0 \pmod{p}$.*

Proof. Write $l=(p-1)/2+k$ (thus k assumes the values $0,\ldots,(p+1)/2$). Put $P_{2i}(x)=(2i)^{2l+2}\prod_{j=1}^{2i}(2i-j+jx)$. Note that the degree of this polynomial equals $2i$. Proceding as in Lemma 11 we infer that, modulo p,

$$\begin{aligned} v_{lp+\frac{p+3}{2}+i} &\equiv \Big[(x-1)(x+\ldots+x^{p-1})^{2l+1}P_{2i}(x)\Big]_{x^{lp+(p+1)/2+i}} \\ &\equiv \Big[(x-1)(x^p+x^{2p}\ldots+x^{p(p-1)})(x+\ldots+x^{p-1})^{2k}P_{2i}(x)\Big]_{x^{lp+(p+1)/2+i}}. \quad (6) \end{aligned}$$

We consider the case $l=p$ (that is $k=(p+1)/2$) first. Then

$$\begin{aligned} v_{lp+\frac{p+3}{2}+i} &\equiv \Big[(x-1)(x^p+x^{2p}+\ldots+x^{p(p-1)})^2(x+\ldots+x^{p-1})P_{2i}(x)\Big]_{x^{lp+(p+1)/2+i}} \\ &= \Big[(x^p-x)(x^p+x^{2p}+\ldots+x^{p(p-1)})^2P_{2i}(x)\Big]_{x^{lp+(p+1)/2+i}}=0, \end{aligned}$$

where we used the observation that the polynomial in brackets has the form

$$\sum_k P_{2i}(x)(c_{kp}x^{kp}+c_{kp+1}x^{kp+1}),$$

and that $1+2i<(p+1)/2+i\le p-1$.

Thus we may assume that $l\le p-1$. Notice that $lp+(p+1)/2+i<p^2$. Furthermore, by Lemma 12 we have $[B_{2k}(x)P_{2i}(x)]_{x^{(l-1)p+(p+1)/2+i}}=0$, as

$$2k-1+2i<(l-1)p+\frac{p+1}{2}+i.$$

Using this, (6) and Lemma 12 we infer that

$$\begin{aligned} v_{lp+\frac{p+3}{2}+i} &\equiv \Big[(x-1)(x^p+\ldots+x^{p(p-1)})(x+\ldots+x^{p-1})^{2k}P_{2i}(x)\Big]_{x^{lp+(p+1)/2+i}} \\ &= \Big[(x-1)(x^p+\ldots+x^{p^2})(x+\ldots+x^{p-1})^{2k}P_{2i}(x)\Big]_{x^{lp+(p+1)/2+i}} \end{aligned}$$

$$
\begin{aligned}
&= \Big[(x-1)(1+\ldots+x^{p(p-1)})(x+\ldots+x^{p-1})^{2k}P_{2i}(x)\Big]_{x^{(l-1)p+(p+1)/2+i}} \\
&= \Big[(x-1)(1+\ldots+x^{p(p-1)})P_{2i}(x)+B_{2k}(x)P_{2i}(x)\Big]_{x^{(l-1)p+(p+1)/2+i}} \\
&= \Big[(x-1)(1+\ldots+x^{p(p-1)})P_{2i}(x)\Big]_{x^{(l-1)p+(p+1)/2+i}} = 0.
\end{aligned}
$$

This concludes the proof. □

A further question concerning the distribution of v_n modulo primes is how frequently certain residues appear. For example, is it true that the zero have density 1 ? Is it true that the non-zero entries are equidistributed ? Questions like this can be answered for the middle binomial coefficient $\binom{2k}{k}$, see e.g. [2, 16, 17]. The following lemma suggests that perhaps techniques from the latter papers can be used to investigate this issue.

Lemma 14 *We have* $v_{1+3k} \equiv v_{2+3k} \equiv \frac{1}{k+1}\binom{2k}{k} \pmod 3$ *and* $v_{3k} \equiv 0 \pmod 3$.

Proof. By Lemma 1 we have $v_{3k} \equiv 0 \pmod 3$. By Lemma 3 we have $v_{1+3k} \equiv v_{2+3k} \pmod 3$. We have, modulo 3,

$$
\begin{aligned}
v_{2+3k} &\equiv \Big[(1-x)\prod_{j=0}^{1+6k}(1-j+jx)\Big]_{x^{1+3k}} = \Big[(1-x)(-x(1+x))^{2k}x\Big]_{x^{1+3k}} \\
&= \Big[(1-x)(1+x)^{2k}\Big]_{x^k} = \binom{2k}{k} - \binom{2k}{k-1} = \frac{1}{k+1}\binom{2k}{k}.
\end{aligned}
$$

This concludes the proof. □

3.3 The sequence $\{v_n\}_{n=1}^{\infty}$ modulo prime powers

The proof of the next lemma was kindly communicated to us by Carl Pomerance.

Lemma 15 *The polynomial* $\prod_{i=0}^{p^l-1}(ix-i+j) \pmod{p^l}$, *as a polynomial in* x, *depends only on the class* $j \pmod p$ *(ie. replacing* j *by* $j+kp$ *would yield the same result).*

Proof. Let $f_j(x) = \prod_{i=0}^{p^r-1}(ix+j)$. If $p|j$, then there are p^{r-1} factors divisible by p and $p^{r-1} \geq r$, so that $f_j(x) \equiv 0 \pmod{p^r}$. So assume $p \nmid j$. Let k be the inverse of j, so $jk \equiv 1 \pmod{p^r}$. Then modulo p^r, we have $f_j(x) \equiv j^{p^r} f_1(x)$ (since the expression ik runs over a complete residue system modulo p^r as i runs). Now say $j \equiv j_1 \pmod p$, say $j_1 = j + kp$. Using induction with respect to r one then easily sees that $j_1^{p^r} = (j+kp)^{p^r} \equiv j^{p^r} \pmod{p^r}$, and we are done. □

Proof of Theorem 2. Part 1. We have

$$
\begin{aligned}
v_{\frac{p+3}{2}} &= p^2\Big[(1-x)\prod_{j=1}^{p-1}(p-j+jx)\Big]_{x^{\frac{p-1}{2}}} \\
&\equiv p^2\Big[(1-x)\prod_{j=1}^{p-1}(-j+jx) + (1-x)p\sum_{k=1}^{p-1}\prod_{\substack{j=1\\ j\neq k}}^{p-1}(-j+jx) \\
&\quad +(1-x)p^2\sum_{1\leq k<r\leq p-1}\ \prod_{\substack{j=1\\ j\neq k,r}}^{p-1}(-j+jx)\Big]_{x^{\frac{p-1}{2}}} \pmod{p^5}
\end{aligned}
$$

$$
\begin{aligned}
&\equiv -p^2(p-1)!\Big[(x-1)^p+(x-1)^{p-1}p\sum_{k=1}^{p-1}\frac{1}{k}\\
&\quad +(x-1)^{p-2}p^2\sum_{1\le k<r\le p-1}\frac{1}{kr}\Big]_{x^{\frac{p-1}{2}}} \pmod{p^5}\\
&\equiv -p^2\{(p-1)!\}\Big[(x-1)^p\Big]_{x^{\frac{p-1}{2}}} \pmod{p^5},\\
&\equiv -p^2\{(p-1)!\}\binom{p}{\frac{p-1}{2}}(-1)^{\frac{p+1}{2}} \pmod{p^5},\\
&\equiv 2p^3\{(p-1)!\}(1-p)\binom{p-1}{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} \pmod{p^5},
\end{aligned}
$$

where we used that $\sum_{k=1}^{p-1} 1/k \equiv 0 \pmod{p^2}$ (this is Wolstenholme's theorem [12, Theorem 115]) and $\sum_{1\le k<r\le p-1} 1/kr \equiv 0 \pmod{p}$. To see the latter congruence note that

$$
(p-1)!\sum_{1\le k<r\le p-1}\frac{1}{kr}=\Big[\prod_{j=1}^{p-1}(x-j)\Big]_{x^{p-3}}\equiv\Big[x^{p-1}-1\Big]_{x^{p-3}}=0 \pmod{p}.
$$

Now it is an easy consequence of Eisenstein's congruence (1859), see [12, Theorem 132], which states that

$$
\frac{2^{p-1}-1}{p}\equiv 1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{p-2} \pmod{p},
$$

that (see ibid. Theorem 133) $\binom{p}{(p-1)/2}(-1)^{\frac{p-1}{2}} \equiv 4^{p-1} \pmod{p^2}$. (Indeed, by Morley's congruence (1895), cf. [4], this congruence is even valid modulo p^3.) We thus finally infer that $v_{\frac{p+3}{2}} \equiv 2p^3(1-p)\{(p-1)!\}4^{p-1} \pmod{p^5}$, which of course implies that $v_{\frac{p+3}{2}} \equiv -2p^3 \pmod{p^4}$.

Part 2. We have the formal series identity

$$
\frac{1}{(1-x)^{2r}}=\sum_{k=0}^{\infty}\binom{k+2r-1}{2r-1}x^k.
$$

Note that

$$
[(x-1)^{-2r}]_{x^{\frac{p-1}{2}-s+rp}}\equiv\frac{(1-2s)_{2r-1}}{2^{2r-1}(2r-1)!} \pmod{p}.
$$

Using the latter congruence we find that, modulo p^{2r+3}.

$$
\begin{aligned}
v_{\frac{p+3}{2}+rp} &= \Big[(1-x)\prod_{j=0}^{(2r+1)p}((2r+1)p-j+jx)\Big]_{x^{\frac{p+1}{2}+rp}}\\
&\equiv p^{2r+2}\Big[(1-x)\prod_{j=0}^{2r+1}(2r+1-j+jx)\prod_{\substack{j=0\\ p\nmid j}}^{(2r+1)p}(-j+jx)\Big]_{x^{\frac{p+1}{2}+rp}}\\
&\equiv (2r+1)^2p^{2r+2}\Big[\Big(\sum_{j=0}^{2r}b_{j,r}x^j\Big)(x-1)^{(2r+1)p-2r}\Big]_{x^{(p-1)/2+rp}}\\
&\equiv (2r+1)^2p^{2r+2}\Big[\Big(\sum_{j=0}^{2r}b_{j,r}x^j\Big)(x-1)^{(2r+1)p}\sum_{k=0}^{\infty}\binom{k+2r-1}{2r-1}x^k\Big]_{x^{(p-1)/2+rp}}
\end{aligned}
$$

$$
\begin{aligned}
&\equiv -(2r+1)^2 p^{2r+2}\Big[\Big(\sum_{j=0}^{2r} b_{j,r}x^j\Big)\sum_{l=0}^{r} x^{lp}(-1)^l \sum_{k=0}^{\infty}\binom{k+2r-1}{2r-1}x^k\Big]_{x^{(p-1)/2+rp}}\\
&\equiv -(2r+1)^2 p^{2r+2}\sum_{l=0}^{r}\binom{2r+1}{l}(-1)^l\sum_{j=0}^{2r} b_{j,r}\binom{\frac{p-1}{2}-j+(r-l)p+2r-1}{2r-1}\\
&\equiv -\frac{(2r+1)^2p^{2r+2}}{2^{2r-1}(2r-1)!}\sum_{l=0}^{r}\binom{2r+1}{l}(-1)^l\sum_{j=0}^{2r} b_{j,r}((1-2j))_{2r-1}\\
&\equiv \frac{(-1)^{r-1}(2r+1)^2}{2^{2r-1}(2r-1)!}\binom{2r}{r}p^{2r+2}\sum_{j=0}^{2r} b_{j,r}((1-2j))_{2r-1}\\
&= C_r p^{2r+2},
\end{aligned}
$$

where in the one but last step we used the identity

$$(-1)^r\binom{2r}{r}=\sum_{l=0}^{r}\binom{2r+1}{l}(-1)^l,$$

which is obtained by comparing the coefficient of x^r of both sides of the identity $(1-x)^{-1}(1-x)^{2r+1}=(1-x)^{2r}$. This finishes the proof. □

3.4 The sequence $\{v_n\}_{n=1}^{\infty}$ modulo powers of two

Before we can consider the sequence modulo powers of two we need some preparatory lemmas.

Lemma 16 *If j is odd, then* $\prod_{i=0}^{2^q-1}(ix-i+j)^2\equiv x^{2^q} \pmod{2^q}$.

Proof. By induction with respect to q. For $q=1$ the result is obvious. Assume the result is established for $1\le q\le q_1$. We write

$$\prod_{i=0}^{2^{q_1+1}-1}(ix-i+j)^2=\prod_{i=0}^{2^{q_1}-1}(ix-i+j)^2\prod_{i=2^{q_1}}^{2^{q_1+1}-1}(ix-i+j)^2=P_1(x)P_2(x),$$

say. Note that $P_1(x)\equiv P_2(x) \pmod{2^{q_1}}$. The induction hypothesis thus implies that we can write $P_1(x)=x^{2^{q_1}}+2^{q_1}f_1(x)$ and $P_2(x)=x^{2^{q_1}}+2^{q_1}f_2(x)$. Since $(ix-i+j)^2\equiv((i+2^{q_1})x-(i+2^{q_1})+j)^2 \pmod{2^{q_1+1}}$, it even follows that $P_1(x)\equiv P_2(x) \pmod{2^{q_1+1}}$, from which we infer that $f_1(x)\equiv f_2(x) \pmod 2$ and hence $f_1(x)+f_2(x)\equiv 0 \pmod 2$. It follows that modulo 2^{q_1+1} the product under consideration equals

$$P_1(x)P_2(x)=(x^{2^{q_1}}+2^{q_1}f_1(x))(x^{2^{q_1}}+2^{q_1}f_2(x))=x^{2^{q_1+1}} \pmod{2^{q_1+1}}.$$

This concludes the proof. □

In the course of the above proof we have showed that

$$\prod_{i=0}^{2^q-1}(ix-i+j)^2\equiv\prod_{i=2^q}^{2^{q+1}-1}(ix-i+j)^2 \pmod{2^{q+1}}.$$

The next result shows that the same identity holds true for the 'square roots'. Using this the 'square root' of the left hand side of Lemma 16 can be computed (Lemma 18).

Lemma 17 *Let j be odd and $q \geq 2$. Then*

$$\prod_{i=0}^{2^q-1}(ix-i+j) \equiv \prod_{i=2^q}^{2^{q+1}-1}(ix-i+j) \pmod{2^{q+1}}.$$

Proof. It is an easy observation that, modulo 2, we have for $0 \leq k \leq 2^q-1$ that

$$\prod_{a=0,\ a\neq k}^{2^q-1}(j-a+ax) \equiv \begin{cases} x^{2^{q-1}-1} & \text{if } k \text{ is odd;} \\ x^{2^{q-1}} & \text{if } k \text{ is even.} \end{cases}$$

Using this identity we find that, modulo 2^{q+1},

$$\begin{aligned}
\prod_{i=2^q}^{2^{q+1}-1}(ix-i+j) &= \prod_{i=0}^{2^q-1}(ix-i+j+2^q(x-1)) \\
&\equiv \prod_{i=0}^{2^q-1}(ix-i+j) + 2^q(x-1)\sum_{k=0}^{2^q-1}\prod_{i=0,\ i\neq k}^{2^q-1}(ix-i+j) \\
&\equiv \prod_{i=0}^{2^q-1}(ix-i+j) + 2^q(x-1)\Big(x^{2^{q-1}}\sum_{2|k}^{2^q-2}1 + x^{2^{q-1}-1}\sum_{2\nmid k}^{2^q-1}1\Big) \\
&\equiv \prod_{i=0}^{2^q-1}(ix-i+j) + 2^q(x-1)(x^{2^{q-1}}2^{q-1} + x^{2^{q-1}-1}2^{q-1}) \\
&\equiv \prod_{i=0}^{2^q-1}(ix-i+j).
\end{aligned}$$

This finishes the proof. □

Lemma 18 *Let j be odd and $q \geq 3$. We have*

$$\prod_{i=0}^{2^q-1}(ix-i+j) \equiv x^{2^{q-1}-2}\Big[2^{q-1}(x^4+x^3+x+1)+x^2\Big] \pmod{2^q}.$$

Proof. Similar to that of Lemma 16, but with the difference that instead of the equality $P_1(x) \equiv P_2(x) \pmod{2^{q+1}}$, we use Lemma 17. □

`Remark`. By Lemma 15 it suffices to work in the proofs of Lemma 16, 17 and 18 with $j = 1$.

The next result established part of parts 8 and 9 of Theorem 1.

Lemma 19 *For $q \geq 1$ we have $v_{2^q} \equiv -1 \pmod{2^q}$.*

Proof. Put $P_q(x) = (1-x)\prod_{j=0}^{2^{q+1}-3}(-3-j+jx)$. We want to compute the coefficient of x^{2^q-1} in $P_q(x)$ modulo 2^q. On invoking Lemma 16 one finds that

$$P_q(x)(1+2x)(2+x) \equiv x^{2^q}(1-x) \pmod{2^q},$$

from which we infer that

$$\begin{aligned}
P_q(x) &\equiv x^{2^q-q}(1-x)\sum_{k=0}^{\infty}(-2)^k x^k \sum_{r=0}^{q-1}(-2)^{q-1-r}x^r \pmod{2^q}\\
&\equiv x^{2^q-q}(1-x)\sum_{m=0}^{2q-2} a_m x^m \equiv x^{2^q-q}\sum_{m=0}^{2q-1} b_m x^m \pmod{2^q},
\end{aligned}$$

where

$$a_m \equiv \begin{cases} -(-2)^{q-1-m}/3 & \text{if } 0\le m\le q-1;\\ -(-2)^{-q+1+m}/3 & \text{if } q\le m\le 2q-2 \end{cases} \textit{ and } b_m \equiv \begin{cases} -(-2)^{q-1-m} & \text{if } 0\le m\le q-1;\\ (-2)^{m-q} & \text{if } q\le m\le 2q-1. \end{cases}$$

Thus $v_{2^q} \equiv b_{q-1} \equiv -1 \pmod{2^q}$. □

Recall that we defined $v_0 = -1$. The reason for this is that this definition allows us to also formulate the next lemma, which together with Lemma 23 is part 8 of Theorem 1, with $j = 0$.

Lemma 20 *(Periodicity.) Suppose that $i, k \ge 0$. We have $v_{k2^q+i} \equiv v_i \pmod{2^q}$.*

Proof. First assume that $i \ge 2$. Note that

$$v_{k2^q+i} \equiv \Big[(1-x)\prod_{j=0}^{2^q-1}(2i-3-j+jx)^{2k}\prod_{j=0}^{2i-3}(2i-3-j+jx)\Big]_{x^{k2^q+i-1}} \pmod{2^q}.$$

By lemma 16, the first product equals x^{k2^q} mod 2^q. Thus

$$v_{k2^q+i} \equiv \Big[(1-x)\prod_{j=0}^{2i-3}(2i-3-j+jx)\Big]_{x^{i-1}} \equiv v_i \pmod{2^q}.$$

In order to deal with the case $i = 1$, we note that, using Lemma 3, $v_{k2^q+1} \equiv v_{k2^q+2} \equiv v_2 \equiv v_1 \pmod{2^q}$. In case $i = 0$ one finds proceding as above that, for $k \ge 1$, $v_{k2^q} \equiv v_{2^q} \pmod{2^q}$. On invoking Lemma 19 it then follows that $v_{k2^q} \equiv v_{2^q} \equiv v_0 \pmod{2^q}$. □

The next result yields a part of part 9 of Theorem 1.

Lemma 21 *Suppose that $q \ge 1$. Then $v_{2^{q-1}} \equiv 2^{q-1} - 1 \pmod{2^q}$.*

Proof. Similar to that of Lemma 19. For $q \le 3$ one verifies the claim numerically. So assume $q \ge 4$. We want to compute the coefficient of $x^{2^{q-1}-1}$ in $P_{q-1}(x)$ modulo 2^q. On invoking Lemma 18 one finds that

$$P_{q-1}(x)(1+2x)(2+x) \equiv x^{2^{q-1}-2}\Big[2^{q-1}(x^4+x^3+x+1)+x^2\Big] \pmod{2^q},$$

whence $P_{q-1}(x) \equiv x^{2^{q-1}-q-2}\Big(\sum_{m=0}^{2q-1} b_m x^m\Big)\Big[2^{q-1}(x^4+x^3+x+1)+x^2\Big] \pmod{2^q}$. (Note that the assumption $q \ge 4$ implies that $2^{q-1}-q-2 \ge 0$.) Thus modulo 2^q the coefficient of $x^{2^{q-1}-1}$, that is $v_{2^{q-1}}$, equals

$$v_{2^{q-1}} \equiv b_{q-1} + 2^{q-1}(b_{q-3}+b_{q-2}+b_q+b_{q+1})$$

$$\equiv \quad -1 + 2^{q-1}(-4+2-2+1) \equiv 2^{q-1} - 1.$$

This completes the proof. $\square$

The next result with $i = 0, 1$ and 2 yields a part of part 9 of Theorem 1. It also yields part 10 of Theorem 1.

Lemma 22 *For $i \ge 0$ and $q \ge 2$ we have $v_{2^{q-1}+i} \equiv v_i + 2^{q-1} \pmod{2^q}$.*

Proof. For $q = 2$ one checks the result numerically and so we may assume $q \ge 3$. For $i = 0$ the result follows by Lemma 21. Note that, a priori, $v_{2^{q-1}+i} \equiv v_i \pmod{2^{q-1}}$ and so either $v_{2^{q-1}+i} \equiv v_i \pmod{2^q}$ or $v_{2^{q-1}+i} \equiv v_i + 2^{q-1} \pmod{2^q}$. Let us first assume that $i \ge 2$. The idea of the proof is to use Lemma 17 to write $v_{2^{q-1}+i} \equiv v_i + 2^{q-1}[f_{q,i}(x)]_{x^{2^{q-1}+i-1}} \pmod{2^q}$. An easy computation then shows that $[f_{q,i}(x)]_{x^{2^{q-1}+i-1}}$ is odd, thus finishing the proof.

More precisely, one first notes that, modulo 2^q,

$$\begin{aligned}
v_{2^{q-1}+i} &\equiv \Big[(1-x)\prod_{j=0}^{2^q-1}(2i-3-j+jx)\prod_{j=2^q}^{2^q+2i-3}(2i-3-j+jx)\Big]_{x^{2^{q-1}+i-1}} \\
&\equiv \Big[(1-x)\prod_{j=0}^{2^q-1}(2i-3-j+jx)\prod_{j=0}^{2i-3}(2i-3-j+jx)\Big]_{x^{2^{q-1}+i-1}} \\
&\equiv \Big[(1-x)x^{2^{q-1}-2}(2^{q-1}(x^4+x^3+x+1)+x^2)\prod_{j=0}^{2i-3}(2i-3-j+jx)\Big]_{x^{2^{q-1}+i-1}} \\
&\equiv v_i + 2^{q-1}\Big[(1-x)(x^4+x^3+x+1)\prod_{j=0}^{2i-3}(2i-3-j+jx)\Big]_{x^{i+1}} \\
&\equiv v_i + 2^{q-1}\Big[(1-x)(x^4+x^3+x+1)x^{i-1}\Big]_{x^{i+1}}
\end{aligned}$$

Since $[(1-x)(x^4+x^3+x+1)x^{i-1}]_{x^{i+1}} = [(1-x)(x^4+x^3+x+1)]_{x^2} = -1$ is odd, the result follows for $j \ge 2$. On combining this result for $i = 2$ and Lemma 3 we find that $v_{2^{q-1}+1} \equiv v_{2^{q-1}+2} \equiv v_2 = v_1 \pmod{2^q}$. Thus the result follows for every $j \ge 0$. $\square$

Using induction and the latter lemma one then easily infers the following result which, together with Lemma 20, gives part 8 of Theorem 1.

Lemma 23 *(Equidistribution.) Let $q \ge 1$. For every odd integer a there are precisely two integers $1 \le j_1 < j_2 \le 2^q$ such that $v_{j_1} \equiv a \pmod{2^q}$ and $v_{j_2} \equiv a \pmod{2^q}$.*

3.5 On a result of Paolo Dominici

Let $S_k(x_1, \ldots, x_r)$ denote the kth elementary symmetric function in r variables, i.e. $S_1(x_1, \ldots, x_r) = x_1 + \ldots + x_r$, $S_2(x_1, \ldots, x_r) = x_1x_2 + x_1x_3 + \ldots + x_{r-1}x_r$, etc.. Paolo Dominici [7] states the following result for v_n without reference.

Theorem 3 *For $1 \le i \le 2n-4$ we put $y_i = i/(2n-3-i)$. Then*

$$v_n = (2n-3)^2(2n-4)!\{S_{n-2}(y_1, \ldots, y_{2n-4}) - S_{n-1}(y_1, \ldots, y_{2n-4})\}.$$

We will now derive this result from (3). We need two lemmas

Lemma 24 *Let $L_1(x),\dots,L_r(x)$ be linear polynomials, then*

$$\frac{1}{m!}\frac{d^m}{dx^m}\{L_1(x)\cdots L_r(x)\} = S_m\left(\frac{L_1'(x)}{L_1(x)},\dots,\frac{L_r'(x)}{L_r(x)}\right)L_1(x)\cdots L_r(x).$$

Another observation we need is the following:

Lemma 25 *Let $x_1,\dots,x_r$ be distinct non-zero elements such that $x_1\cdot x_2\cdots x_r=1$ and $\{x_1,\dots,x_r\}=\{\frac{1}{x_1},\dots,\frac{1}{x_r}\}$. Then $S_{r-k}(x_1,\dots,x_r)=S_k(x_1,\dots,x_r)$, with $1\le r\le k$.*

Proof. Note that $S_{r-k}(x_1,\dots,x_r)=S_k(\frac{1}{x_1},\dots,\frac{1}{x_r})x_1\cdots x_r=S_k(x_1,\dots,x_r)$, where in the derivation of the first equality we used the assumption that $x_i\neq 0$ and in that of the second the remaining assumptions. □

Corollary 1 *For $1\le k\le 2n-5$ we have $S_k(y_1,\dots,y_{2n-4})=S_{2n-4-k}(y_1,\dots,y_{2n-4})$.*

Proof of Theorem 3. Put $P_n(x)=\prod_{j=1}^{2n-4}(2n-3-j+jx)$. By definition we have

$$v_n=\Big[(1-x)\prod_{j=0}^{2n-3}(2n-3-j+jx)\Big]_{x^{n-1}}=(2n-3)^2\Big[(1-x)P_n(x)\Big]_{x^{n-2}}.$$

Thus,

$$v_n=(2n-3)^2\{[P_n(x)]_{x^{n-2}}-[P_n(x)]_{x^{n-3}}\}. \tag{7}$$

On noting that $[P_n(x)]_{x^m}=\frac{1}{m!}\frac{d^m}{dx^m}P_n(x)|_{x=0}$, we obtain on invoking Lemma 24 that

$$[P_n(x)]_{x^m}=(2n-4)!S_m(y_1,\dots,y_i,\dots,y_{2n-4}). \tag{8}$$

Combining (8) with (7) yields that

$$v_n=(2n-3)^2(2n-4)!\{S_{n-2}(y_1,\dots,y_{2n-4})-S_{n-3}(y_1,\dots,y_{2n-4})\},$$

or, on invoking Corollary 1,

$$v_n=(2n-3)^2(2n-4)!\{S_{n-2}(y_1,\dots,y_{2n-4})-S_{n-1}(y_1,\dots,y_{2n-4})\},$$

This concludes the proof. □

From the above proof we infer that we may alternatively define v_n by

$$v_n=\Big[(x-1)\prod_{j=0}^{2n-3}(2n-3-j+jx)\Big]_{x^n}. \tag{9}$$

We leave it to the reader to use the observation that $P(x):=\prod_{j=1}^{2n-4}(2n-3-j+jx)$ is selfreciprocal, i.e. satisfies $P(1/x)x^{2m-4}=P(x)$ to infer (9) directly from (3).

Many of the congruences can be also proved using Theorem 3. As an example we will show that if p is an odd prime, then $v_{3(p+1)/2}\equiv -81p^4 \pmod{p^5}$. This is the case $r=1$ of part 2 of Theorem 2.

Proof of part 2 of Theorem 2 in case $r=1$. Set $n = 3(p+1)/2$. Note that $(2n-3)^2(2n-4)! \equiv -18p^4 \pmod{p^5}$. It thus remains to be proven that the expression in braces in Theorem 3 equals $9/2$ modulo p. It turns out to be a little easier to work with $w_i = -y_i$. Note that $(-1)^r S_r(w_1, \ldots, w_{3p-1}) = S_r(y_1, \ldots, y_{3p-1})$. We have $w_i = i/(i-3p)$ for $1 \le i \le 3p-1$. Thus $w_p = -1/2$, $w_{2p} = -2$ and the remaining w_i satisfy $w_i \equiv 1 \pmod{p}$. Hence $S_r(w_1, \ldots, w_{3p-1}) \equiv S_r(-1/2, -2, 1, 1, \ldots, 1) \pmod{p}$, where $2 \le r \le 3p-1$. In the symmetric function $S_r(z_1, \ldots, z_{3p-1})$ there are $\binom{3p-3}{r}$ terms containing neither z_1 nor z_2. There are $\binom{3p-3}{r-1}$ terms containing z_1, but not z_2. Finally there are $\binom{3p-3}{r-2}$ terms containing both z_1 and z_2. It follows that, modulo p,

$$(-1)^r S_r(y_1, \ldots, y_{3p-1}) \equiv S_r(-\frac{1}{2}, -2, 1, \ldots, 1) = \binom{3p-3}{r} - (2+\frac{1}{2})\binom{3p-3}{r-1} + \binom{3p-3}{r-2}.$$

Modulo p we have

$$\begin{aligned}
(-1)^n \quad & \{S_{n-2}(y_1, \ldots, y_{2n-4}) - S_{n-1}(y_1, \ldots, y_{2n-4})\} \\
\equiv \quad & \binom{3p-2}{n-1} - \frac{5}{2}\binom{3p-2}{n-2} + \binom{3p-2}{n-3} \\
\equiv \quad & 2\binom{p-2}{n-p-1} - 5\binom{p-2}{n-p-2} + 2\binom{p-2}{n-p-3} \\
\equiv \quad & \left[2\binom{p-2}{n-p-1} + 4\binom{p-2}{n-p-2} + 2\binom{p-2}{n-p-3}\right] - 9\binom{p-2}{n-p-2} \\
\equiv \quad & \left[2\binom{p}{n-p-1}\right] - 9\binom{p-2}{n-p-2} \\
\equiv \quad & -9\binom{p-2}{n-p-2} \equiv (-1)^n 9(n-p-1) \equiv (-1)^n \frac{9}{2}.
\end{aligned}$$

This completes the proof. □

4 Asymptotics

Given a sequence of coefficients, there are many things we would like to know about it. Apart from the search for a generating function and for a recursion formula, an interesting question is the asymptotic behaviour. We remind the reader that candidate Fourier series for modular forms of weight $2k$ for $SL(2, \mathbb{Z})$ must have coefficients growing like n^{2k-1} (and n^k for cusp forms).

In our case, without prior knowledge of the alternative definition (3), we only managed to compute the first 80 values of v_n using the *Schubert* package for intersection theory [13] or the first 225 values using the rational function (with the dummy variables w_i). Numerically, it is readily seen that the leading term for the v_n is $e^{2n \log n}$. As this is strongly reminiscent of the behaviour of $(2n)! = \exp(2n\log(2n) - 2n + \frac{1}{2}\log 2n + \frac{1}{2}\log 2\pi + O(\frac{1}{n}))$, we rather study the behaviour of $\log \frac{v_n}{(2n)!}$ and find now the leading term to be $2n$. Subtracting it, we find the next-to-leading term to be $-4\log n$, easily verified by applying $n\partial_n$ (ie. taking subsequent differences and multiplying by n). The next term is a constant, $C = -5.62...$, which we find difficult to recognize. We have learnt from Don Zagier a smart technique which enables to determine a large number of digits of C; we present it below under the name of asymp$_k$ trick.

4.1 The asymp_k trick

Assume we are given numerically a few hundred terms of a sequence $s = \{s_n\}_{n\in\mathbb{N}}$ which we believe has an asymptotic expansion goes in inverse powers of n, ie.

$$s_n \sim c_0 + \frac{c_1}{n} + \frac{c_2}{n^2} + \dots .$$

Goal: determine the coefficients c_i numerically.
Trick: Choose some moderate value of k (say $k = 8$) and define a new sequence $s^{(k)}$ as $\frac{1}{k!}\Delta^k N^k s$, where Δ is the difference operator $(\Delta u)_n = u_n - u_{n-1}$ and N the multiplication operator $(Nu)_n = nu_n$, i.e.,

$$s_n^{(k)} = \sum_{j=0}^{k} \frac{(-1)^j}{j!\,(k-j)!}\,(n-j)^k\, s_{n-j}\,.$$

For n large we have (assuming the above asymptotic expansion for s itself)

$$s_n^{(k)} = c_0 + (-1)^k \frac{c_{k+1}}{n^{k+1}} + (-1)^k \frac{\left((k+1)c_{k+2} - \binom{k+1}{2}c_{k+1}\right)}{n^{k+2}} + \dots .$$

Thus, while s_n approximates c_0 only to within an accuracy $O(n^{-1})$, $s_n^{(k)}$ approximates it to the much better accuracy $O(n^{-k})$, so we obtain a very good approximation for c_0. Call this operation $\underline{\text{asymp}_k}$. The further coefficients c_i are then obtained inductively: if $c_0, \dots, c_{i-1}$ are known to high precision, we get c_i by applying asymp_k to the sequence $n^i(s_n - c_0 - \cdots - c_{i-1}/n^{i-1}) = c_i + c_{i+1}/n + \cdots$.

The crucial point in the success of asymp_k is that the operator Δ^k sends n^k to $k!$ and kills polynomials of degree $< k$, so that all the intermediate terms of the expansion of s_n between c_0 and $c_k n^{-k}$ disappear.

Variants of asymp_k allow one to deal for example with asymptotic expansions of the form

(I) $s_n \sim A\log n + c_0 + c_1/n + c_2/n^2 + \cdots$

(II) $s_n \sim Bn + A\log n + c_0 + c_1/n + c_2/n^2 + \cdots$

(III) $s_n \sim An^\lambda(1 + c_1/n + c_2/n^2 + \cdots)$

In case (I) we can apply asymp_k to the sequence $n(s_{n+1} - s_n)$, which has the form $A + c_1'/n + c_2'/n^2 + \cdots$, to obtain A to high precision, after which we apply the original method to $\{s_n - A\log n\}$. In case (II) we apply asymp_k twice to Δs to get B and A, and then subtract (our approximation for) $B\log n + A$ from s_n and apply the standard version. For case (III) we can either look at $\{\log s_n\}$ and apply variant (I) or else apply asymp_k to $\{n(s_{n+1}/s_n - 1)\}$ to get λ and then apply the standard method to $\{s_n/n^\lambda\}$.

`Remark 1`. Applying the operation asymp_k with suitably chosen k gives a rapidly convergent sequence $s^{(k)}$. To estimate how many decimals are probably correct, we look at some relatively widely spaced elements of this sequence (e.g., the terms $s_n^{(k)}$ with $n = 300$, 400, 500 if we know 500 terms of the sequence s) and see how many of their digits agree.

Remark 2. One also has to experiment to find the optimal choice of k. Typically one uses $k = 5$ if one knows 200 terms of s and $k = 8$ if one knows 1000 terms. This suggests that perhaps $k \approx \log N$ is a good choice for a generic sequence with N computed terms.

Remark 3. The asymp_k trick was first described in a paper of Zagier [21]. Here he considers the Stoimenov numbers ξ_D which bound the number $V(D)$ of linearly indepedent Vassiliev invariants of degree D. Stoimenov himself thought that ξ_D behaves 'something like $D!/1.5^D$'. Calculating the values up to $D = 200$ and applying a variation of asymp_k suggested an asymptotic formula of the form

$$\xi_D \sim \frac{D!\sqrt{D}}{(\pi^2/6)^D}\left(C_0 + \frac{C_1}{D} + \frac{C_2}{D^2} + \cdots\right),$$

with $C_0 \approx 2.704332490062429595$, $C_1 \approx -1.52707$ and $C_2 \approx -0.269009$. Subsequently Zagier was able to prove this with explicitly computable constants C_i. In particular, $C_0 = 12\sqrt{3}\pi^{-5/2}e^{\pi^2/12}$, which agrees to the accuracy given above with the empirically obtained value.

4.2 Application to the asymptotics of v_n

In our case of sequence v_n of lines in a hypersurface of $\mathbb{P}^n$, the coefficients $c_0 =: C$ is difficult to recognize, but all other coefficients, $c_1, c_2, \ldots$ are rational numbers which we easily recognize from a sufficient number of digits. Once the first few rational coefficients have been found and the corresponding terms subtracted from the sequence s, the constant term C can be obtained with 30 digits, say. This is enough to feed to the PARI software and apply the function `lindep([C,1,log(Pi),log(2),log(3)])` to find a rational linear combination of C in terms of a given basis (educated guess). The result, equivalent to (4) is:

$$\log\frac{v_n}{(2n)!} = 2n - 4\log n + C + \frac{11}{6n} + \frac{141}{160n^2} + \ldots, \tag{10}$$

where $C := -3 - \log\pi - \frac{3}{2}\log\frac{8}{3}$. In the appendix we present a proof by Don Zagier of this asymptotic formula.

5 Comparison with two other sequences

As a matter of curiosity, we now compare our results so far with similar results from two other sequences of enumerative geometry. We shall see that the first case has quite similar features, while the second case is more intricate.

5.1 Numbers of plane rational curves

One sequence of integers from enumerative geometry is n_d, the number of plane rational curves of degree d through $3d-1$ points in $\mathbb{P}^2$. Kontsevich's recursion formula [14] reads

$$n_d = \sum_{k=1}^{d-1} n_k\, n_{d-k}\left[k^2(d-k)^2\binom{3d-4}{3k-2} - k^3(d-k)\binom{3d-4}{3k-1}\right], \qquad n_1 = 1.$$

The result is $n_1 = 1$, $n_2 = 1$, $n_3 = 12$, etc, ie. there is 1 line through 2 points of the plane, 1 conic through 5 points of the plane, 12 cubics through 8 points of the plane, etc.

We can similarly draw tables of $n_d \bmod k$ for any integer k. The results (in the same convention as before) are:

* $k = 2$: both rows vanish (except first two values), ie. all n_d are even.
* $k = 2^l$: all rows are 0, ie $n_d \equiv 0 \bmod 2^l$ for $n > l + 1$.
* $k = 3$: $n_{3d} \equiv 0 \bmod 3$, $n_{3d+2} \equiv 1 \bmod 3$, $n_{3d+1} \equiv$ alternating 1 or 2 mod 3 because $n_{6d+2} \equiv 4 \bmod 6$.
* $k = 5$: $n_d \equiv 0 \bmod 5$, for $d > 8$. Idem for $k = 25$ ($d > 23$)

Because of this big symmetry for low primes, most non-primes will yield constant or regular rows (ie rows repeating when shifting horizontally). The only non-obvious case is $k = 26$, where there is a shift by 8 (because $k = 13$ shifts by 16) and rows 4,6 alternate with 0.

Further, we only found three primes with regular features:

* $k = 7$: all rows are regular (repeat when shifted horizontally by 4), rows 5 and 7 are 0.
* $k = 13$: idem, shift by 16, no 0 row.
* $k = 19$: idem, shift by 12, no 0 row.
* $k = 5, 11, 17, 23, 29$: these primes give almost-0 rows (ie. $n_d \equiv 0$ except for a finite number of d).

We have not attempted to prove these observations.

5.1.1 Asymptotics

We now turn to the asymptotics of the sequence n_d for $d \to \infty$. Di Francesco and Itzykson proved [6, Proposition 3] that

$$\frac{n_d}{(3d-1)!} \;=\; \frac{A^d}{d^{7/2}}\left(B + \mathrm{O}(\frac{1}{d})\right),$$

as d tends to infinity, and found the approximate values $A \approx 0.138$ and $B \approx 6.1$ for the constants A and B. Assuming a full asymptotic expansion

$$\frac{n_d}{(3d-1)!} \;\sim\; \frac{A^d}{d^{7/2}}\left(B_0 + \frac{B_1}{d} + \frac{B_2}{d^2} + \cdots\right),$$

and applying variant (II) of the asymp_k trick to $\log(n_d/(3d-1)!)$, we obtain the much more accurate approximations

$$\begin{aligned} A &\approx 0.138009346634518656829562628891755541716014121072\,, \\ B_0 &\approx 6.0358078488159024106383768720948935\,, \end{aligned}$$

as well as the further values $B_1 \approx -2.2352424409362074$, $B_2 \approx 0.054313787925$. Unfortunately, we are not able to recognize any of these apparently irrational numbers, e.g., PARI does not see in $\log A$ and $\log B_0$ a linear combination of simple numbers like 1, $\log 2$, $\log 3$, $\log \pi$, π and π^2.

5.2 Numbers of rational curves on the quintic threefold

The other sequence we now introduce for the purpose of comparison is q_d, that of holomorphic rational curves of degree d embedded in the quintic Calabi-Yau threefold. These are the 'instanton numbers' of Candelas et al [5]. They are defined by the following line:

$$5+\sum_{n\geq 1} q_n\, n^3 \frac{q^n}{1-q^n} = \left(\frac{q}{x}\frac{dx}{dq}\right)^3 \frac{5}{(1-5^5x)\; y_0(x)^2} = 5+2875\; q+4876875\; q^2+\ldots, \quad (11)$$

where $q(x) = x\; e^{\tilde{y}_1/y_0} = x + 770\; x^2 + \ldots$ is the "mirror map" and its inverse is $x(q) = q - 770\; q^2 + \ldots$. The functions y_0 and $\tilde{y}_1$ are solutions of a Picard-Fuchs differential equation and are given by

$$y_0(x) := \sum_{n\geq 0} \frac{(5n)!}{n!^5}\; x^n \qquad \text{and} \qquad \tilde{y}_1(x) = \sum_{n\geq 0} \left(\frac{(5n)!}{n!^5}\; 5 \sum_{j=n+1}^{5n} \frac{1}{j}\right)\; x^n.$$

When computing the numbers q_d, the longest step is without doubt the inversion of the series $q(x)$. The first few values are $q_1 = 2875$, $q_2 = 609250$, etc.

We can again draw tables of q_d mod k for any integer k. The main results (in the same convention as before) are:

* $k = 2$: second row is 0, ie. q_{2d} are even.
* $k = 4, 8, 16$: last row is 0, ie. $q_{2^l d} \equiv 0 \bmod 2^l$ $(l \leq 4)$
* $k = 8, 16$: rows 4,8,12,... are also 0, ie. $q_{2^l d+4m} \equiv 0 \bmod 2^l$ $(l \leq 4)$
* $k = 32$: no 0 rows anymore!
* $k = 5$: all rows are 0, idem at $k = 25$.
* $k = 20$: row 4,8,12,16,20 are 0, because both are 0 mod 4 and mod 5.

These congruences are much less impressive than in the previous cases, due to the more complicated origin of the instantons. It is not even mathematically understood why these are integers and what exactly they count. Again we have not attempted to prove the congruences.

5.2.1 Asymptotics

In this case the asymptotic behaviour is much more tricky than in the previous two examples. The growth is indeed exponential, but $\log q_d$ has more than a simple logarithmic term and monomial terms. Indeed, subtracting the logarithmic term gives us a sequence on which the asymp_k trick works badly – as if other logarithmic terms were hiding. In fact, finding out the coefficient of the first log term is already quite tough, and differentiating (to get rid of log-terms) does not yield anything with only monomials. The second author's attempts to deal with the asymptotics of $\log q_d$ through the asymp_k trick can be found in [11].

6 Conclusion

Though the congruences satisfied by the sequence v_n of lines in $\mathbb{P}^n$ are numerous and very interesting, the exponential asymptotic growth $v_n \sim n^{2n}$ rules out that the v_n are

Fourier coefficients of any modular form on a subgroup of $SL(2,\mathbb{Z})$ (whose coefficients typically grow like n^{2k-1} for weight $2k$). It is quite gratifying to see that the asymptotic expansion in (10) can be written out with as many exact terms as one wishes, since the coefficients are rational.

Another sequence – that of numbers n_d of degree d curves through $3d-1$ points of the plane – has very similar behaviour, in terms of congruences as well as asymptotics (though the latter's coefficients will be irrational and not recognized). A last sequence – that of numbers q_d of degree d rational curves on the quintic Calabi-Yau threefold – is much less enticing; its congruences are rather limited and its asymptotics are awkward: not simply one or two log-terms followed by mere monomial terms, but certainly log(log) terms or infinitely many log terms.

It would be interesting to study more of typical sequences from enumerative geometry and see if there is an underlying pattern. Also, the question of how many of those sequences satisfy a recurrence relation is still open. Among the three sequences that we discussed, only that of n_d (plane rational curves) obeys a known recurrence.

Acknowledgments

The first author, who initiated this paper, is deeply grateful for Don Zagier's help throughout all the stages of this project. Not only did Don simplify matters considerably with his formula (3), but he also equipped him with the asymp$_k$ trick. He is thankful for fruitful discussions with Robert Osburn. The second author likes to thank Daniel Berend, Paolo Dominici and Yossi Moshe for interesting e-mail correspondence and Carl Pomerance for providing us with Lemma 15. He especially likes to thank Don Zagier for his help in improving the exposition of the paper. Dmitry Kerner and Masha Vlasenko we thank for several helpful discussions. Several inaccuracies in an earlier version were detected by Alexander Blessing during a two week practicum he did with the second author.

This project was made possible thanks to the support of the MPIM in Bonn.

APPENDIX

by Don Zagier

Exact and asymptotic formulas for v_n

In this appendix we prove the alternative definition (3) and the asymptotic formulae (4) and (10) for the numbers v_n defined in (2).

Exact formulas

Proposition 1 *Let $G(x,y)$ be a homogeneous polynomial of degree $2n$ in two variables and $P(x)$ a monic polynomial of degree $n+1$ with distinct roots. Then the expression*

$$\sum_{\substack{\alpha,\,\beta\in\mathbb{C}\\ P(\alpha)=P(\beta)=0}} \frac{G(\alpha,\beta)}{P'(\alpha)P'(\beta)} \tag{12}$$

is independent of P and equals the coefficient of $x^n y^n$ in $G(x,y)$.

Proof. By linearity it is enough to consider monomials $G(x,y) = x^r y^s$, $r+s=2n$. Then the expression (12) factors as $(\sum_{P(\alpha)=0} \frac{\alpha^r}{P'(\alpha)})(\sum_{P(\beta)=0} \frac{\beta^s}{P'(\beta)})$. But by the residue theorem we have

$$\sum_{P(\alpha)=0} \frac{\alpha^r}{P'(\alpha)} = \sum_{\alpha\in\mathbb{C}} \mathrm{Res}_{x=\alpha}\Big(\frac{x^r\,dx}{P(x)}\Big) = -\mathrm{Res}_{x=\infty}\Big(\frac{x^r\,dx}{P(x)}\Big),$$

and this equals 0 if $0 \le r < n$ and 1 if $r = n$ since P is monic of degree $n+1$. The proposition follows. $\square$

`Remark.` The same proof shows that if G is homogeneous of degree $m+n$ and P and Q are two monic polynomials of degrees $m+1$ and $n+1$ with distinct roots, then

$$\sum_{P(\alpha)=Q(\beta)=0} \frac{G(\alpha,\beta)}{P'(\alpha)Q'(\beta)}$$

is independent of P and Q and is equal to the coefficient of $x^m y^n$ in $G(x,y)$. Yet more generally, and still with the same proof, if G is a homogeneous polynomial of degree $n_1+\cdots+n_k$ in k variables and $P_1,\ldots,P_k$ monic polynomials of degree $n_1+1,\ldots,n_k+1$ with no multiple roots, then

$$\sum_{P_1(\alpha_1)=\ldots=P_k(\alpha_k)=0} \frac{G(\alpha_1,\ldots,\alpha_k)}{P_1'(\alpha_1)\cdots P_k'(\alpha_k)}$$

is independent of all the P_i and is equal to the coefficient of $x_1^{n_1}\cdots x_k^{n_k}$ in $G(x_1,\ldots,x_k)$. In fact G need not even be homogeneous, but can be any polynomial in k variables of degree $\le n_1+\cdots+n_k$.

Corollary 2 *Let $F(x,y)$ be a symmetric homogeneous polynomial of degree $2n-2$ in two variables and $w_0,\ldots,w_n$ distinct complex numbers. Then the expression*

$$\sum_{0\le i<j\le n} \frac{F(w_i,w_j)}{\prod\limits_{\substack{0\le k\le n\\ k\ne i,\,j}} (w_i-w_k)(w_j-w_k)}$$

is independent of $w_0,\ldots,w_n$ and equals the coefficient of x^{n-1} in $(1-x)F(x,1)$.

Proof. This follows after a short calculation if we apply the proposition to $G(x,y) = (x-y)^2F(x,y)$, $P(x) = \prod_{i=0}^n (x-w_i)$. $\square$

Corollary 2 immediately implies that the right hand side of equation (2) is independent of the (distinct) complex variables $w_0,\ldots,w_n$ and that (2) is equivalent to (3). The computational advantage is huge: formula (2) is very slow to compute, even for moderately large n, whereas (3) can be implemented in PARI in one line as

```
v(n) = coeff(prod(j=0,2*n-3,2*n-3-j+j*x,1-x),n-1)
```

and takes < 2 seconds to compute v_n up to $n = 100$ and 46 seconds up to $n = 224$.

We can rewrite (3) in several other forms by using residue calculus. Setting $D=2n-3$ and making the substitution $x=1-D/z$, we find

$$v_n = \operatorname{Res}_{x=0}\Bigl((1-x)\prod_{j=0}^{2n-3}(2n-3-j+jx)\,\frac{dx}{x^n}\Bigr) \tag{13}$$

$$= D^{2n}\,\operatorname{Res}_{z=D}\Bigl(\frac{\prod_{j=0}^{D}(z-j)}{z^{n+1}\,(z-D)^n}\,dz\Bigr). \tag{14}$$

Since the residue of the integrand at infinity is zero, we can also write this as

$$v_n = -\,D^{2n}\,\operatorname{Res}_{z=0}\Bigl(\frac{\prod_{j=0}^{D}(z-j)}{z^{n+1}\,(z-D)^n}\,dz\Bigr), \tag{15}$$

while simply making the substitution $z\mapsto D-z$ in (14) gives the similar expression

$$v_n = D^{2n}\operatorname{Res}_{z=0}\Bigl(\frac{\prod_{j=0}^{D}(z-j)}{z^{n}\,(z-D)^{n+1}}\,dz\Bigr), \tag{16}$$

and adding these two last expressions gives yet a third form:

$$v_n = \frac{1}{2}D^{2n+1}\operatorname{Res}_{z=0}\Bigl(\frac{\prod_{j=0}^{D}(z-j)}{z^{n+1}\,(z-D)^{n+1}}\,dz\Bigr). \tag{17}$$

Each of the formulae (15)–(17) expresses v_n as the constant term at $z=0$ of the Laurent expansion of a rational function, e.g. (15) says

$$v_n = (-1)^n D^{2n}\cdot\text{coefficient of } z^{n-1} \text{ in } \tfrac{(1-z)(2-z)\cdots(D-1-z)}{(D-z)^{n-1}} \text{ as } z\to 0. \tag{18}$$

Substituting $z=Du$, we can write this as

$$v_n = (-1)^n D^{2}\cdot\text{coefficient of } u^{n-1} \text{ in } \tfrac{(1-Du)(2-Du)\cdots(D-1-Du)}{(1-u)^{n-1}} \text{ as } u\to 0, \tag{19}$$

from which we see again that $D^2|v_n$ (Lemma 1). By expanding $(D-z)^{1-n}$ by the binomial theorem, we also obtain closed formulae for v_n; for instance (18) gives:

$$v_n = \sum_{m=0}^{n-1}(-1)^{n-1-m}\binom{2n-2-m}{n-1}D^{m+1}\begin{bmatrix}D\\m\end{bmatrix}, \tag{20}$$

where $\begin{bmatrix}D\\m\end{bmatrix}$, the coefficient of z^m in $z(z+1)\cdots(z+D-1)$, is a Stirling number of the first kind.

Asymptotics

To obtain the asymptotic expansion of v_n, we write the residue in (13) as $\frac{1}{2\pi i}\int_{|x|=1}$ and we make the substitution $x=(1+it)/(1-it)$ to obtain, after a short calculation,

$$v_n = \frac{2}{\pi}\int_{-\infty}^{\infty}\prod_{r=1,3,\dots,D}\Bigl(\frac{D^2+r^2t^2}{1+t^2}\Bigr)\frac{t^2\,dt}{(1+t^2)^2} = \frac{2}{\pi}D^{D+1}\int_{-\infty}^{\infty}\phi_D(t)\frac{t^2\,dt}{(1+t^2)^2}, \tag{21}$$

where $\phi_D(t)$ denotes the rational function

$$\phi_D(t) = \prod_{r=1,3,\ldots,D} \frac{1+r^2D^{-2}t^2}{1+t^2}.$$

It is easy to see that $\phi_D(0) = 1$ and $\phi_D(t) \le e^{-cDt^2}$ for some absolute constant $c > 0$ (a much more precise formula will be given in a moment), so the main contribution to the integral comes from small t. For t small and D large we have (uniformly in both variables)

$$\begin{aligned}
\log\phi_D(t) &= \sum_{j=1}^{\infty} \frac{(-1)^{j-1}}{j} \Big[\sum_{r=1,3,\ldots,D} \Big(\frac{r^{2j}}{D^{2j}} - 1\Big)\Big] t^{2j} \\
&= \Big(-\frac{D}{3} + \frac{1}{3D}\Big) t^2 + \Big(\frac{D}{5} - \frac{1}{3D} + \frac{2}{15D^3}\Big) t^4 + \Big(-\frac{D}{7} + \frac{1}{3D} - \frac{4}{9D^3} + O\Big(\frac{1}{D^5}\Big)\Big) t^6 \\
&+ \Big(\frac{D}{9} - \frac{1}{3D} + \frac{14}{15D^3} + O\Big(\frac{1}{D^5}\Big)\Big) t^8 + \Big(-\frac{D}{11} + \frac{1}{3D} + O\Big(\frac{1}{D^3}\Big)\Big) t^{10} \\
&+ \Big(\frac{D}{13} - \frac{1}{3D} + O\Big(\frac{1}{D^3}\Big)\Big) t^{12} + \Big(-\frac{D}{15} + O\Big(\frac{1}{D}\Big)\Big) t^{14} + \Big(\frac{D}{17} + O\Big(\frac{1}{D}\Big)\Big) t^{16} + O(Dt^{18}),
\end{aligned}$$

and hence

$$\begin{aligned}
&\frac{x^2}{(1+x^2/D)^2}\,\phi_D\big(\frac{x}{\sqrt{D}}\big) \\
&= e^{-x^2/3}\Big[x^2 + \Big(\frac{x^6}{5} - 2x^4\Big)D^{-1} + \Big(\frac{x^{10}}{50} - \frac{19x^8}{35} + 3x^6 + \frac{x^4}{3}\Big)D^{-2} \\
&+ \Big(\frac{x^{14}}{750} - \frac{12x^{12}}{175} + \frac{314x^{10}}{315} - \frac{59x^8}{15} - x^6\Big)D^{-3} + \cdots \\
&+ \Big(\frac{x^{30}}{393750000} - \frac{11x^{28}}{19687500} + \cdots + \frac{355x^{10}}{162} + \frac{2x^8}{45}\Big)D^{-7} + O(D^{-8})\Big].
\end{aligned}$$

Substituting this expansion (with the 34 omitted terms included) into equation (21) with t replaced by $x/\sqrt{D}$ and using the standard evaluation

$$\int_{-\infty}^{\infty} e^{-x^2/3} x^{2n}\,dx = \frac{(2n)!}{n!}\Big(\frac{3}{4}\Big)^n \sqrt{3\pi},$$

we obtain

$$\begin{aligned}
v_n \;=\; &\sqrt{\frac{27}{\pi}} D^{D-1/2}\Big(1 - \frac{9}{4}D^{-1} + \frac{969}{160}D^{-2} - \frac{61479}{3200}D^{-3} + \frac{25225773}{358400}D^{-4} \\
&- \frac{10092025737}{35840000}D^{-5} + \frac{2271842858513}{2007040000}D^{-6} - \frac{4442983688169}{1146880000}D^{-7} + O(D^{-8})\Big).
\end{aligned}$$

This asymptotic formula can of course be written in many other ways, e.g.:

$$v_n = \sqrt{\frac{27}{\pi}}(2n-3)^{2n-7/2}\Big(1 - \frac{9}{8n} - \frac{111}{640n^2} - \frac{9999}{25600n^3} + \frac{87261}{5734400n^4} - \cdots\Big)$$

or

$$v_n = e^{-3}\sqrt{\frac{27}{\pi}}(2n)^{2n-7/2}\Big(1 + \frac{15}{8n} + \frac{1689}{640n^2} + \frac{79281}{25600n^3} + \frac{19691853}{5734400n^4} + \cdots\Big)$$

or

$$\log \frac{v_n}{(2n)!} = 2n - 4\log n + C + \frac{11}{6n} + \frac{141}{160n^2} + \frac{9973}{28800n^3} + \frac{59673}{179200n^4} + \cdots$$

with $C = -3 - \log\pi - \frac{3}{2}\log\frac{8}{3}$. Of course, more terms could be obtained in any of these expansions if desired.

References

[1] F.L. Bauer, For all primes greater than 3, $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ holds, *Math. Intelligencer* **10** (1988), no. 3, 42.

[2] D. Berend and J.E. Harmse, On some arithmetical properties of middle binomial coefficients, *Acta Arith.* **84** (1998), 31–41.

[3] F. Beukers, Irrationality proofs using modular forms, Astérisque No. **147-148** (1987), 271–283.

[4] T. Cai, A congruence involving the quotients of Euler and its applications. I, *Acta Arith.* **103** (2002), 313–320.

[5] P. Candelas, J.X. de la Ossa, P. Green, and L. Parkes, *A Pair of Calabi-Yau Manifolds as an Exactly Soluble Superconformal Field Theory*, Nucl. Phys. **B359** (1991), 21–74, reprinted in *Essays on Mirror Manifolds* (S.T. Yau, ed.) Hong Kong, 1992.

[6] P. Di Francesco and C. Itzykson, Quantum intersection rings. *The moduli space of curves* (Texel Island, 1994), 81–148, Progr. Math., 129, Birkhäuser Boston, Boston, MA, 1995.

[7] P. Dominici, Sequence A027363, *On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`.

[8] W. Fulton, *Intersection Theory*, Springer, New York, 1984.

[9] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, *Organic mathematics* (Burnaby, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.

[10] D. Grünberg, Integrality of open instanton numbers, *J. Geom. Phys.* **52** (2004), 284–297, hep-th/0305057.

[11] D. Grünberg, *Asymptotic growth of the sequence of instantons on the quintic threefold*, unpublished manuscript, 2005.

[12] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers.* Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[13] S. Katz and S.A. Stromme, *Schubert -a Maple package for intersection theory and enumerative geometry*, (1992) `http://www.mi.uib.no/~stromme/schubert/`

[14] M. Kontsevich and Y. Manin, Gromov-Witten classes, quantum cohomology, and enumerative geometry, *Comm. Math. Phys.* **164** (1994), 525–562, hep-th/9402147.

[15] L. Manivel, *Symmetric functions, Schubert polynomials and degeneracy loci*, SMF/AMS Texts and Monographs **6**, American Mathematical Society, Providence, RI, 2001.

[16] Y. Moshe, The density of 0's in recurrence double sequences, *J. Number Theory* **103** (2003), 109–121.

[17] Y. Moshe, The distribution of elements in automatic double sequences, *Discrete Math.* **297** (2005), 91–103.

[18] J. Stienstra and F. Beukers, On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces, *Math. Ann.* **271** (1985), 269–304.

[19] B.L. van der Waerden, Zur algebraischen Geometrie. II. Die geraden Linien auf den Hyperflächen des $\mathbb{P}_n$. *Math. Ann.* **108** (1933), 253–259.

[20] B.L. van der Waerden, *Zur algebraischen Geometrie. Selected papers*, Springer-Verlag, Berlin, 1983.

[21] D. Zagier, Vassiliev invariants and a strange identity related to the Dedekind eta-function, *Topology* **40** (2001), 945–960.

D. Grünberg, 49 rue Fondary, 75015 Paris, e-mail: grunberg@mccme.ru

P. Moree, Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.

e-mail: moree@mpim-bonn.mpg.de

D. Zagier, Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.

e-mail: don@mpim-bonn.mpg.de