INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A47

FACTORIZATION OF CONSTANTS INVOLVED IN CONJECTURAL MOMENTS OF ZETA-FUNCTIONS

Jam Germain
Université de Montréal, Montréal, Canada
jamgermain@gmail.com

Received: 9/13/2008, Accepted: 10/14/2008, Published: 10/27/08

Abstract

We give the factorization of certain constants that appear in (conjectural) formulas for moments of zeta-functions, making it obvious that these constants are integers (which was already proved by Conrey and Farmer). We extend this analysis to other constants emerging from the random-matrix theory calculations of Keating and Snaith.

1. Introduction.

Following work of Conrey and Ghosh, and of Keating and Snaith [6], it is believed that

$$\frac{1}{T}\int_0^T \left|\zeta\left(\frac{1}{2}+it\right)\right|^{2k} \sim g_{k,U}\cdot\prod_p\left(\left(1-\frac{1}{p}\right)^{k^2}\sum_{j\geq 0}\frac{d_k(p^j)^2}{p^j}\right)\cdot\frac{(\log T)^{k^2}}{k^2!} \tag{1}$$

where $\zeta(s)^k=\sum_{n\geq 1}\frac{d_k(n)}{n^s}$, and

$$g_{k,U} := (k^2)!\ \frac{1!2!\dots(k-1)!}{k!(k+1)!\dots(2k-1)!}\ . \tag{2}$$

This has been proved for $k=1$ (Hardy and Littlewood, 1918) and $k=2$ (Ingham, 1926), and is otherwise an open conjecture. The lower bound $\gg_k (\log T)^{k^2}$ was given by Ramachandra [7] in 1980, and with the implicit constant as in (1), divided by $g_{k,U}$, assuming the Riemann Hypothesis by Conrey and Ghosh [3] in 1984, and the upper bound $\ll_{k,\epsilon} (\log T)^{k^2+\epsilon}$ assuming the Riemann Hypothesis was given recently by Soundararajan [10]. A persuasive heuristic argument in favour of (1) is given in [2].

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

Similarly one can conjecture the average value of the "$2k$th moments" of other L-functions, perhaps averaging over different L-functions in a certain class (for example the quadratic Dirichlet L-functions, or those connected with natural classes of modular forms) rather than over t. Various cases have been considered, following the philosophy of Katz and Sarnak [5], especially as formulated in [2], and each involves a formula like (1), though with slightly different constants involved. In fact the power of $\log T$ involved, and the Euler product have long been understood since they come from number theoretic considerations. The highly influential work of Keating and Snaith [6] suggests a value for the constants g_k in each case, coming from a random matrix theory calculation, namely the average of the sth power of the absolute value of the characteristic polynomial of an $N \times N$ matrix as we vary over a suitable set of matrices (with an appropriate measure).[1] Lower bounds for these moments, out by at most a constant, were given by Rudnick and Soundararajan [8,9], and good upper bounds, out by at most $(\log T)^{o(1)}$, by Soundararajan [10, section 4].

The first few $g_{k,U}$ are $1, 2, 42, 24024, \ldots$ and seem to always be integers, though this is not clear from the definition (2). Conrey and Farmer [1] confirmed the experimental evidence that these are always integers, and even noticed some self-similar structure in the powers to which primes divide these integers.[2] We give another proof of the fact that these are always integers by obtaining a new description of the power to which each prime divides g_k, which also easily explains (and confirms) Conrey and Farmer's observations about self-similarity.

For a given integer k and prime power q we define k_q to be that integer satisfying $k_q \equiv k \pmod{q}$ with $-q/2 \le k_q < q/2$. We let $[t]$ be the largest integer $\le t$, and $\{t\} = t - [t] \in [0, 1)$ be the fractional part of t.

Theorem 1_U. *We have*

$$g_{k,U} := (k^2)! \, \frac{1!2! \ldots (k-1)!}{k!(k+1)! \ldots (2k-1)!} \; = \prod_{\substack{p \text{ prime} \\ a \ge 1, \; q = p^a}} p^{\left[\frac{k_q^2}{q}\right]} ,$$

so that $g_{k,U}$ is an integer for all $k \ge 1$.

Conrey and Farmer also showed that the numbers

$$g_{k,Sp} := 2^{\frac{1}{2}k(k+1)} \left(\frac{k(k+1)}{2}\right)! \, \frac{1!2! \ldots k!}{2!4! \ldots 2k!} .$$

are all integers, and we give our own proof:

[1] For example, the 'U' in $g_{k,U}$ stands for the set of unitary matrices, taken with Haar measure.
[2] They also gave a complete history of the conjectured existence and study of these constants g_k.

Theorem 1_{Sp}. *We have*

$$g_{k,Sp}/2^{\frac{1}{2}k(k+1)} = \prod_{\substack{p \text{ prime } \geq 3 \\ a\geq 1,\ q=p^a}} p^{\left[\frac{k_q(k_q+1)}{2q}\right]} \cdot \prod_{a\geq 1,\ q=2^a} 2^{\left[\frac{k_q(k_q+1)}{2q} - \frac{1}{2}\left(\left[\frac{2k}{q}\right]-\left[\frac{k}{q}\right]\right)\right]},$$

so that $g_{k,Sp}/2^{\frac{1}{2}k(k-1)}$ is an integer for all $k \geq 1$.

The main idea in the proof goes back to Legendre and Kummer, and is widely used when understanding prime factors of binomial coefficients (see, e.g., [4]): Write out each factorial $j!$ as the product of the integers up to j and then determine how many of these integers are divisible by each prime power q. One pieces that information together to get the result.[3]

Jon Keating suggested looking at [6] for other constants that might prove to be integers, when multiplied through by a suitable quantity. There are several natural ways to guess at "suitable". Here we give one which generalizes the last part of Theorem 1_U:

Theorem 2_{even}. *The number*

$$G_{m,k} := (mk^2)! \cdot \frac{(mk)!}{k!^m} \cdot \frac{m!\ 2m!\ 3m! \ldots (k-1)m!}{km!\ (k+1)m! \ldots (2k-1)m!}$$

is an integer for any integers $m, k \geq 1$.

Note that $g_{k,U} = G_{1,k}$ so this generalizes Theorem 1_U. It almost gives Theorem 1_{Sp}: Since $(2!\ 4! \ldots 2l!)^2 = (2!\ 4! \ldots 2l!)(1!2\ 3!4 \ldots (2l-1)!2l) = (1!\ 2!\ 3! \ldots 2l!)2^l l!$,

$$G_{2,k} = (2k^2)! \cdot \frac{(2k)!}{k!^2} \cdot \frac{(2!\ 4!\ 6! \ldots 2(k-1)!)^2}{2!\ 4!\ \ldots 2(2k-1)!} = (2k^2)! \cdot \frac{2^k}{k!} \cdot \frac{1!\ 2!\ 3! \ldots (2k-1)!}{2!\ 4!\ \ldots 2(2k-1)!}$$
$$= \binom{2k^2}{k} \cdot \frac{g_{2k-1,Sp}}{2^{2k^2-2k}}$$

so these are closely related.

We will give a further (but more complicated) generalization, Theorem 2_{odd}, in Section 4.

Theorem 2 does not give a factorization comparable to those given in Theorem 1. Actually it is possible to do so with additional complications since, in general, the exponent on q will equal l^2/qm where l is the least residue, in absolute value, of $mk \pmod q$ plus a term which depends only on $q \pmod m$ and $[2mk/q] \pmod{2m}$, but which does not obviously yield a simple description (see Corollary 5.3 below).

[3]Note that if j is divisible by p^ℓ we count the ℓ powers of p by including them one at a time, since j is divisible by p, then since j is divisible by p^2, ... , and finally since j is divisible by p^ℓ.

Notation: Here and henceforth $(t)_d$ is the least non-negative residue of $t \pmod d$, and note that $\{\frac{t}{d}\} = \frac{(t)_d}{d}$. As usual $v_p(m)$ denotes the power of p that divides m. Let $\omega_q(a_1 \cdot a_2 \cdots a_r)$ denote the number of a_j that are divisible by q.[4] Also $\omega_q(a \cdot b!) = \omega_q(a \cdot 1 \cdot 2 \cdots b)$, and note that $\omega_q(b!) = [b/q]$. The key observation (as described above) is that

$$v_p(a_1 \cdot a_2 \cdots a_r) = \sum_{\substack{e \geq 1 \\ q=p^e}} \omega_q(a_1 \cdot a_2 \cdots a_r).$$

2. Proof of Theorem 1.

Proof of the factorization of $g_{k,U}$. For $n = aq + b$ with $0 \leq b \leq q-1$, the number of integers amongst $1!2!\ldots(aq+b)!$ that are divisible by q, that is $\omega_q(1!2!\ldots n!)$, is

$$\sum_{i=0}^{n} \left[\frac{i}{q}\right] = \sum_{i=0}^{n} \frac{i}{q} - \left\{\frac{i}{q}\right\} = \frac{n(n+1)}{2q} - \sum_{j=0}^{a-1}\sum_{\ell=0}^{q-1} \frac{\ell}{q} - \sum_{\ell=0}^{b} \frac{\ell}{q} = \frac{n(n+1)}{2q} - a \cdot \frac{q-1}{2} - \frac{b(b+1)}{2q}.$$

Writing $k-1 = aq+b$, so that $2k-1 = Aq+B$ with $A = 2a, B = 2b+1$ if $b \leq \frac{q}{2} - 1$, and $A = 2a+1, B = 2b+1-q$ if $b > \frac{q}{2} - 1$, we deduce that $\omega_q(g_{k,U})$ equals

$$\frac{k^2}{q} - \left\{\frac{k^2}{q}\right\} + 2\left(\frac{k(k-1)}{2q} - a \cdot \frac{q-1}{2} - \frac{b(b+1)}{2q}\right) - \left(\frac{2k(2k-1)}{2q} - A \cdot \frac{q-1}{2} - \frac{B(B+1)}{2q}\right)$$
$$= (A-2a) \cdot \frac{q-1}{2} + \frac{B(B+1)}{2q} - \frac{b(b+1)}{q} - \left\{\frac{(b+1)^2}{q}\right\}.$$

Now if $b+1 \leq \frac{q}{2}$ then this is

$$\frac{(b+1)^2}{q} - \left\{\frac{(b+1)^2}{q}\right\} = \left[\frac{(b+1)^2}{q}\right],$$

and if $b+1 > \frac{q}{2}$ then this is

$$q - 2(b+1) + \frac{(b+1)^2}{q} - \left\{\frac{(b+1)^2}{q}\right\} = \frac{(q-(b+1))^2}{q} - \left\{\frac{(b+1)^2}{q}\right\} = \left[\frac{(b+1-q)^2}{q}\right].$$

Proof of the factorization of $g_{k,Sp}$. Now $\omega_q(g_{k,Sp}/2^{\frac{1}{2}k(k+1)})$ equals

$$\left[\frac{k(k+1)}{2q}\right] + \sum_{j=1}^{k} \left[\frac{j}{q}\right] - \left[\frac{2j}{q}\right] = -\left\{\frac{k(k+1)}{2q}\right\} + \sum_{j=1}^{k} \left\{\frac{2j}{q}\right\} - \left\{\frac{j}{q}\right\}$$

[4] Note that this definition depends on the representation, as a product, of the number inside the brackets, and not on the number itself. Hence $\omega_4(2 \cdot 8) = 1$, whereas $\omega_4(4 \cdot 4) = 2$.

If q is odd, then as j runs from one multiple of q to the next, the last two summands run through the same terms and so cancel. Hence if $k = aq + b$ the above becomes

$$-\left\{\frac{b(b+1)}{2q}\right\} + \sum_{j=1}^{b} \frac{2j}{q} - \frac{j}{q} - \sum_{q/2 \le j \le b} 1 = \frac{b(b+1)}{2q} - \left\{\frac{b(b+1)}{2q}\right\} - \max\left\{0, b - \left[\frac{q-1}{2}\right]\right\}.$$

So if $b \le \frac{q-1}{2}$ this equals $\left[\frac{b(b+1)}{2q}\right]$. The result follows for $b > \frac{q-1}{2}$ since

$$\frac{b(b+1)}{2q} - \left(b - \frac{q-1}{2}\right) = \frac{(b-q)(b+1-q)}{2q}.$$

If q is even then

$$\sum_{j=1}^{q} \left\{\frac{2j}{q}\right\} - \left\{\frac{j}{q}\right\} = \sum_{j=1}^{q} \frac{j}{q} - \left(\frac{q}{2}+1\right) = -\frac{1}{2}.$$

There is a new subtlety: $\frac{k(k+1)}{2q} = \frac{b(b+1)}{2q} - \frac{a}{2} \pmod 1$. Hence if $b < \frac{q}{2}$ then we have, in total,

$$\frac{b(b+1)}{2q} - \frac{a}{2} - \left\{\frac{b(b+1)}{2q} - \frac{a}{2}\right\} = \left[\frac{k_q(k_q+1)}{2q} - \frac{a}{2}\right].$$

On the other hand $\frac{k(k+1)}{2q} = \frac{(b-q)(b-q+1)}{2q} - \frac{a+1}{2} \pmod 1$ so that if $b \ge \frac{q}{2}$ then we have, in total,

$$\begin{aligned} &\frac{b(b+1)}{2q} - \left\{\frac{k(k+1)}{2q}\right\} - \left(b - \left(\frac{q}{2} - 1\right)\right) - \frac{a}{2} \\ &= \frac{(b-q)(b-q+1)}{2q} - \frac{a+1}{2} - \left\{\frac{(b-q)(b-q+1)}{2q} - \frac{a+1}{2}\right\} \\ &= \left[\frac{k_q(k_q+1)}{2q} - \frac{a+1}{2}\right]. \end{aligned}$$

Proof that $g_{k,U}$ and $g_{k,Sp}$ are both integers. The exponent corresponding to each prime power is a non-negative integer, except perhaps for the power of 2 in $g_{k,Sp}$. In that case we write $k = \sum_i \delta_i 2^i$ in binary and suppose that $q = 2^e$ with $k = aq + b$, so that $a = \sum_{i \ge e} \delta_i 2^{i-e}$ and $b = \sum_{0 \le i \le e-1} \delta_i 2^i$, and thus $b \ge q/2$ iff $\delta_{e-1} = 1$. Then

$$\begin{aligned} \left[\frac{k_q(k_q+1)}{2q} - \frac{1}{2}\left(\left[\frac{2k}{q}\right] - \left[\frac{k}{q}\right]\right)\right] &= \left[\frac{k_q(k_q+1)}{2q} - \frac{1}{2}\left(\sum_{i \ge e} \delta_i 2^{i-e} + \delta_{e-1}\right)\right] \\ &= \left[\frac{k_q(k_q+1)}{2q} - \frac{1}{2}\left(\delta_{e-1} + \delta_e\right)\right] - \sum_{i \ge e+1} \delta_i 2^{i-e-1}. \end{aligned}$$

Now

$$\sum_{e \ge 1} \sum_{i \ge e+1} \delta_i 2^{i-e-1} = \sum_{i \ge 2} \delta_i \sum_{e=1}^{i-1} 2^{i-1-e} = \sum_{i \ge 1} \delta_i (2^{i-1} - 1) = \left[\frac{k}{2}\right] - \sum_{i \ge 1} \delta_i,$$

so that

$$v_2(g_{k,Sp}) = \frac{k(k+1)}{2} - \left[\frac{k}{2}\right] + \sum_{e\geq 1}\left[\frac{k_q(k_q+1)}{2q} + \frac{1}{2}\left(\delta_e - \delta_{e-1}\right)\right]$$
$$\geq \frac{k^2}{2} + \frac{\delta_0}{2} + \sum_{e\geq 1}\left[\frac{\delta_e - \delta_{e-1}}{2}\right] \geq \frac{k^2}{2} - \frac{\log 2k}{\log 4} \geq \frac{k(k-1)}{2}.$$

3. Further remarks on divisibility of $g_{k,U}$.

3.1. Self-similarity. Let $\| t \| := \min_{n\in\mathbb{Z}} |t-n|$ be the distance from t to the nearest integer. Evidently $|k_q| = q \| k/q \|$ so that $k_q^2/q = q \| k/q \|^2$, and $[k_q^2/q] = q \| k/q \|^2 + O(1)$. Moreover if $q \geq 2k$ then $|k_q| = |k|$ and so if $q > k^2$ then $[k_q^2/q] = 0$. Also if $q > k^2$ then $q \| k/q \|^2 = k^2/q$. From all this we deduce that the power of p dividing $g_{k,U}$, given by $v_p(g_{k,U})$, satisfies

$$\left| v_p(g_{k,U}) - \sum_{a\in\mathbb{Z}} p^a \| k/p^a \|^2 \right| \leq \sum_{\substack{a\geq 1\\ p^a\leq k^2}} 1 + \sum_{\substack{a\geq 1\\ p^a > k^2}} k^2/p^a + \frac{1}{4}\sum_{a\leq 0} p^a \leq \left[\frac{2\log k}{\log p}\right] + \frac{5}{4}\cdot\frac{p}{p-1}.$$

So define, as in [1],

$$c_p(x) = x^{-1}\sum_{a\in\mathbb{Z}} p^a \| x/p^a \|^2,$$

which is “self-similar” in that $c_p(x) = c_p(px)$ for all real x; and so

$$v_p(g_{k,U}) = kc_p(k) + O\left(\frac{\log pk}{\log p}\right) = kc_p(x_{p,k}) + O\left(\frac{\log pk}{\log p}\right), \tag{3.1}$$

where $x_{p,k}$ is the unique element of $[1,p)$ for which $k/x_{p,k}$ is a power of p. This is a strong version of the ingenious Theorem 6.1 of [1].

3.2. Change in p-divisibility. Along these lines it is also interesting to consider $v_p(g_{k+p^b,U}) - v_p(g_{k,U})$ when $p^b \leq k < p^{b+1}$: By (3.1) this equals

$$\sum_{\substack{ae\geq 1\\ q=p^a}} \frac{(k')_q^2 - k_q^2}{q} + O\left(\frac{\log pk}{\log p}\right),$$

where $k' = k + p^b$. Now $k'_q = k_q$ for all $q = p^a,\ a \leq b$, and $k'_q = k'$ with $k_q = k$ provided $k' \leq \frac{q}{2}$ where $q = p^a$. If this holds for $a = b+1$ then the sum above equals

$$\sum_{a\geq b+1} \frac{(k')^2 - k^2}{q} = \frac{k+k'}{p-1}.$$

Otherwise we must make a correction when $q = p^{b+1}$ with $k' > q/2$, in which case either $k < \frac{q}{2}$ whence $k'_q = q - k' = q - p^b - k$ and $k_q = k$, or $\frac{q}{2} < k$ whence $|k'_q| = |q - k'| = |q - p^b - k|$ and $k_q = q - k$. Therefore

$$v_p(g_{k+p^b,U}) - v_p(g_{k,U}) = \frac{k+k'}{p-1} + O\left(\frac{\log pk}{\log p}\right) - 2 \cdot \begin{cases} 0 & \text{if } k' < \frac{q}{2} \\ k' - \frac{p^{b+1}}{2} & \text{if } k < \frac{q}{2} < k' \\ p^b & \text{if } \frac{q}{2} < k \end{cases} .$$

3.3. Further divisibility. The numbers $g_{k,U}$ are highly composite and one might suspect that they are divisible by factorials (in terms of k). A little experimenting and one finds that $g_{k,U}$ is not always divisible by $k!$ but it is close, that is the denominator of $g_{k,U}/k!$ is always small. (Indeed $g_k/k!$ is an integer for $k \leq 4$ but $g_5/5!$ has denominator 2).

For any k there exists r such that $p^r \leq k < p^{r+1}$.

Suppose $k \leq p^{r+1}/2$; then $k_q^2 = k^2$ for $q = p^a$ with $a \geq r+1$, and so $k_q^2/p^{r+b} = k/p^r \cdot k/p^b \geq k/p^b$. Hence, by Theorem 1, the power of p dividing $g_{k,U}$ is

$$\sum_{a\geq 1,\ q=p^a} \left[\frac{k_q^2}{q}\right] \geq \sum_{\substack{b\geq 1 \\ q=p^{r+b}}} \left[\frac{k_q^2}{p^{r+b}}\right] \geq \sum_{b\geq 1} \left[\frac{k}{p^b}\right] = v_p(k!).$$

Now suppose that $k = p^{r+1} - l$ with $l < p^{r+1}/2$. Then $k_q^2 = k^2$ for $q = p^a$ with $a \geq r+2$ (so the same argument as above works for those terms) and $k_q^2 = l^2$ for $q = p^{r+1}$. If $l \geq p^{r+1/2}$ then $l^2/p^{r+1} \geq p^r \geq k/p$ so that

$$\sum_{a\geq 1,\ q=p^a} \left[\frac{k_q^2}{q}\right] \geq \left[\frac{l^2}{p^{r+1}}\right] + \sum_{b\geq 2} \left[\frac{k^2}{p^{r+b}}\right] \geq \sum_{b\geq 1} \left[\frac{k}{p^b}\right] = v_p(k!).$$

Hence the only remaining range is $p^{r+1} - p^{r+1/2} < k < p^{r+1}$, in which we do have examples where p divides the denominator: Let $k = p^2 - p + r$ where $1 \leq r < \sqrt{p}$, so that the power of p dividing $g_{k,U}$ is $[r^2/p] + [(p-r)^2/p^2] + [(p^2-p+r)^2/p^3] = 0 + 0 + p - 2 + [((2r+1)p^2 - 2rp + r^2)/p^3] = p - 2$ whereas $v_p(k!) = [(p^2 - p + r)/p] = p - 1$. In fact one can show that if $k = p^{2r} - p^{2r-1} + p^{2r-2} - p^{2r-3} + \ldots$, where p is sufficiently large (in terms of r) then $v_p(k!) = v_p(g_{k,U}) + r$

We might compensate as follows: Given k, let $\ell_k := 1 + [\sqrt{k}]$. We conjecture that $k!/\ell_k!$ divides $g_{k,U}$, when $k \neq 20, 22$. If true this is "best possible" in that p divides the denominator of $g_{k,U}/(k!/[\sqrt{k}]!)$ when $k = p^2 - p + 1$.

4. Other constants from random matrix theory.

4.1. The big picture: a suggestion of Jon Keating. The average of the sth power of the absolute value of the characteristic polynomial of an $N \times N$ matrix in the various ensembles (Unitary $r = 2$, Orthogonal $r = 1$, Symplectic $r = 4$) is given by the formula (see (110) of [6])

$$M_N(r, s) := \prod_{j=0}^{N-1} \frac{\Gamma(1 + jr/2)\Gamma(1 + s + jr/2)}{\Gamma(1 + s/2 + jr/2)^2}.$$

This product has a lot of cancelation if s is divisible by r, that is $s = rk$ for some integer $k \geq 1$, whence the above becomes

$$\begin{aligned} M_N(r, rk) &= \prod_{j=0}^{N-1} \frac{\Gamma(1 + jr/2)\Gamma(1 + (2k + j)r/2)}{\Gamma(1 + (k + j)r/2)^2} \\ &= P(r, rk) \prod_{j=0}^{k-1} \frac{\Gamma(1 + (N + k + j)r/2)}{\Gamma(1 + (N + j)r/2)} = P(r, rk) \left(\frac{rN}{2}\right)^{rk^2/2} e^{O(k^3/N)}, \end{aligned}$$

where

$$P(r, rk) := \prod_{j=0}^{k-1} \frac{\Gamma(1 + jr/2)}{\Gamma(1 + (k + j)r/2)} . \tag{4.1}$$

Hence as $N \to \infty$,

$$M_N(r, rk) \sim P(r, rk) \left(\frac{rN}{2}\right)^{rk^2/2} .$$

If r is even, say $r = 2m$ we have

$$P(2m, 2mk) = \frac{m!\ 2m!\ 3m! \ldots (k - 1)m!}{km!\ (k + 1)m! \ldots (2k - 1)m!} , \tag{4.2}$$

and so

$$M_N(2m, 2mk) \sim \gamma_{m,k} \frac{N^{mk^2}}{(mk^2)!} \quad \text{where } \gamma_{m,k} := m^{mk^2}(mk^2)! \cdot P(2m, 2mk).$$

In Theorem 1_U we saw that $\gamma_{1,k} = g_{k,U}$, and we might guess that $\gamma_{m,k}$ is always an integer. However this is not so, as we can see from the example $\gamma_{4,k}$ which has denominator $2k - 1$ for $k = 2, 3, 4, 6$. Quite extensive calculations appear to reveal that the denominator of $\gamma_{m,k}$ is always quite small. In section 6 below we will prove Theorem 2_{even}, which states that

$$(mk^2)! \cdot \frac{(mk)!}{k!^m} \cdot P(2m, 2mk) \quad \text{is an integer for any } m, k \geq 1$$

(and hence $\frac{(mk)!}{k!^m} \cdot \gamma_{m,k}$ is always an integer); and we give reasons there to believe that it is unlikely that a smaller multiplier than $\frac{(mk)!}{k!^m}$ will do.

Suppose that r is odd. Note that if d is odd then $\Gamma(1+d/2) = \sqrt{\pi}d!/(2^d[\frac{d}{2}]!)$, so that

$$\prod_{j=0}^{2l-1} \Gamma(1+jr/2) = \prod_{i=0}^{l-1} \Gamma(1+ir)\Gamma(1+(2i+1)r/2) = \prod_{i=0}^{l-1} (ir)! \frac{\sqrt{\pi}(2i+1)r!}{2^{(2i+1)r}\left[\frac{(2i+1)r}{2}\right]!}.$$

Therefore

$$\begin{aligned} P(r,2rk) &= \frac{\prod_{j=0}^{2k-1} \Gamma(1+jr/2)^2}{\prod_{j=0}^{4k-1} \Gamma(1+jr/2)} = 2^{2rk^2} \frac{\prod_{i=0}^{k-1} (ir)!^2(2i+1)r!}{\prod_{i=k}^{2k-1} (ir)!^2(2i+1)r!} \cdot \frac{\prod_{j=2k}^{4k-1} \left[\frac{jr}{2}\right]!}{\prod_{j=0}^{2k-1} \left[\frac{jr}{2}\right]!} \\ &= 2^{2rk^2} \left(\frac{\prod_{i=0}^{k-1} ir!}{\prod_{i=k}^{2k-1} ir!} \right)^2 \cdot \frac{\prod_{i=k}^{2k-1} 2ir!}{\prod_{i=0}^{k-1} 2ir!} \cdot \frac{\prod_{j=0}^{2k-1} jr!}{\prod_{j=2k}^{4k-1} jr!} \cdot \frac{\prod_{j=2k}^{4k-1} \left[\frac{jr}{2}\right]!}{\prod_{j=0}^{2k-1} \left[\frac{jr}{2}\right]!} \\ &= 2^{2rk^2} \cdot \frac{P(2r,2rk)^2 P(2r,4rk)}{P(4r,4rk)} \cdot \frac{\prod_{j=2k}^{4k-1} \left[\frac{jr}{2}\right]!}{\prod_{j=0}^{2k-1} \left[\frac{jr}{2}\right]!}. \end{aligned} \tag{4.3}$$

which is thus a rational number. In section 6 we deduce from (4.3):

Theorem 2_{odd}. *The number*

$$(2rk^2)! \cdot \frac{(rk)!}{k!^r} \cdot \left(\frac{(2rk)!}{k!^{2r}} \right)^2 \cdot \frac{P(r,2rk)}{2^{2rk^2}}$$

is an integer, for any integers $k \geq 1$ and odd $r \geq 1$.

4.2. Connections between constants.

We have seen that $\gamma_{1,k} = g_{k,U}$. There are two ways to obtain $g_{k,Sp}$: For $m = 2$ we have, since $(2j)! = 2j \cdot (2j-1)!$,

$$\begin{aligned} \gamma_{2,k} &= 2^{2k^2}(2k^2)! \cdot \frac{(2!\ 4!\ \ldots (2k-2)!)^2}{2!\ 4!\ \ldots (4k-2)!} \\ &= 2^{2k^2}(2k^2)! \cdot \frac{1!2!3!4!\ldots (2k-2)!(2 \cdot 4 \cdots 2(k-1))}{2!\ 4!\ \ldots (4k-2)!} \\ &= 2^{2k^2}(2k^2)! \cdot \frac{1!2!3!4!\ldots (2k-2)!(2^{k-1} \cdot (k-1)!)}{2!\ 4!\ \ldots (4k-2)!} \\ &= 2^{2k} \frac{(2k^2)!k!}{(2k^2-k)!(2k)!} \cdot g_{2k-1,Sp} \end{aligned}$$

If $r = 1$ we use the identity $\Gamma(z)\Gamma(z+1/2) = 2^{1-2z}\sqrt{\pi}\ \Gamma(2z)$, to obtain

$$\begin{aligned} M_N(1,2k) &\sim \left(\frac{N}{2}\right)^{2k^2} \cdot \prod_{i=0}^{k-1} \frac{\Gamma(1+i)\Gamma(3/2+i)}{\Gamma(1+k+i)\Gamma(3/2+k+i)} \\ &= \left(\frac{N}{2}\right)^{2k^2} \cdot \prod_{i=0}^{k-1} \frac{2^{2k}\Gamma(2+2i)}{\Gamma(2+2i+2k)} \\ &= N^{2k^2} \cdot \frac{1!3!\ldots (2k-1)!}{(2k+1)!(2k+3)!\ldots (4k-1)!} \\ &= \frac{N^{2k^2}}{(2k^2)!} \cdot \frac{(2k^2)!(2k)!^2}{(2k^2-k)!k!(4k)!2^{2(k^2-k)}} \cdot g_{2k-1,Sp}, \end{aligned}$$

so that

$$P(1,2k)=\frac{2^{2k}}{\binom{4k}{2k}}\cdot\frac{g_{2k-1,Sp}}{(2k^2-k)!k!}\quad\text{and}\quad P(4,4k)=\frac{2^{2k-2k^2}}{\binom{2k}{k}}\cdot\frac{g_{2k-1,Sp}}{(2k^2-k)!k!}.$$

Hence Theorems 1_{Sp}, 2_{even} and 2_{odd} imply that

$$2^{k-1}\cdot\frac{g_{2k-1,Sp}}{2^{2k^2-2k}},\quad\binom{2k^2}{k}\cdot\frac{g_{2k-1,Sp}}{2^{2k^2-2k}}\quad\text{and}\quad\binom{2k^2}{k}\cdot\frac{\binom{2k}{k}^2}{\binom{4k}{2k}}\cdot\frac{g_{2k-1,Sp}}{2^{2k^2-2k}}$$

are integers, respectively. This allows us to compare the strength of the various results, and implies that, perhaps, the $(mk^2)!$ and $(2rk^2)!$ in Theorem 2 could be replaced by somethings slightly smaller.

A general identity of this kind is:

$$\begin{aligned}M_{2n-1}(1,s)&=\frac{\Gamma(1+s)}{\Gamma(1+s/2)^2}\cdot\prod_{j=1}^{2n-2}\frac{\Gamma(1+j/2)\Gamma(1+s+j/2)}{\Gamma(1+s/2+j/2)^2}\\&=\frac{4\Gamma(s)}{s\Gamma(s/2)^2}\cdot\prod_{i=1}^{n-1}\frac{\Gamma(\frac12+i)\Gamma(\frac12+s+i)}{\Gamma(\frac12+s/2+i)^2}\cdot\frac{\Gamma(1+i)\Gamma(1+s+i)}{\Gamma(1+s/2+i)^2}\\&=\frac{4\Gamma(s)}{s\Gamma(s/2)^2}\Big/\frac{\Gamma(1+2s)}{\Gamma(1+s)^2}\cdot\prod_{i=0}^{n-1}\frac{\Gamma(1+2i)\Gamma(1+2s+2i)}{\Gamma(1+s+2i)^2}\\&=\frac{2\Gamma(s)^3}{\Gamma(2s)\Gamma(s/2)^2}\cdot M_n(4,2s).\end{aligned}\tag{4.4}$$

5. A reciprocity law.

5.1. A reciprocity law and useful formulas. Define

$$A(n,q;Q):=\#\{i,\ 1\le i\le n:\ (iQ)_q\le(-nQ)_q\}-\frac{n(-nQ)_q}{q}.$$

Theorem 5.1. *Let q and m be coprime integers. For any given integer k, let $n=(k)_q$ and l be the least residue, in absolute value, of mk (mod q),[5] and then $N=\frac{mn-l}{q}$ (which is the nearest integer to mn/q). We have*

$$\omega_q\left((mk^2)!\cdot\frac{m!\ 2m!\ 3m!\dots(k-1)m!}{km!\ (k+1)m!\dots(2k-1)m!}\right)$$

equals

$$A(n,q;m)-\begin{cases}1 & \text{if } n>q/2\\ 0 & \text{otherwise}\end{cases}+\begin{cases}1 & \text{if } l<0\\ 0 & \text{otherwise}\end{cases}-\left\{\frac{mn^2}{q}\right\}.$$

One can directly evaluate $A(n,q;Q)$ though this will not be useful in our application. Instead we have the following "reciprocity law":

[5] If $k\equiv q/2\pmod q$ then we let $l=q/2$.

Proposition 5.2. (Reciprocity law) *Let q and Q be coprime integers. For any given integer $n, 0 \leq n \leq q-1$, let l be the least residue, in absolute value, of $Qn \pmod q$, and then $N = \frac{Qn-l}{q}$ (which is the nearest integer to Qn/q). Let L be the least residue, in absolute value, of $qN \pmod Q$. Then*

$$A(n,q;Q) + A(N,Q;q) = qQ\left|\frac{n}{q} - \frac{N}{Q}\right|^2 - \begin{cases} 1 & \text{if } l, L < 0 \\ 0 & \text{otherwise} \end{cases} + \begin{cases} 1 & \text{if } n > q/2 \\ 0 & \text{otherwise.} \end{cases} \tag{5.1}$$

Although we have attempted to state Proposition 5.2 in as symmetric a form as possible, one cannot interchange the capital and lower case letters, since $n = \frac{qN+l}{Q}$, not $\frac{qN-L}{Q}$, and L is the least residue, in absolute value, of $-l \pmod Q$ so that L can equal $-l$ but not usually.

By combining Theorem 5.1 and Proposition 5.2, we deduce

Corollary 5.3. *With the notation as above we have*

$$\frac{mk^2}{q} + \omega_q(P(2m, 2mk)) = \frac{l^2}{qm} - A(N,m;q) \; + \begin{cases} 1 & \text{if } l < 0 \leq L \\ 0 & \text{otherwise.} \end{cases}$$

One can use Proposition 5.2 to develop an algorithm to evaluate $A(n, q; Q)$:

Algorithm 5.4. For evaluating $A(n, q; Q)$ when $q > Q$ with $(q, Q) = 1$: *Let $q_1 = q$ and $q_2 = Q$. Then let $q_j = r_j q_{j+1} + q_{j+2}$ for each $j \geq 1$, where $r_j = [q_j/q_{j+1}]$ and $q_{j+2} = (q_j)_{q_{j+1}}$; that is $\{q_j : j \geq 1\}$ is the sequence of numbers which appears in the Euclidean algorithm starting with $q > Q$.*

Let $n_1 = n$. Now select n_{j+1} so that n_{j+1}/q_{j+1} is the nearest fraction to n_j/q_j, with denominator q_{j+1}. In the case that n_j/q_j is exactly halfway between two such fractions, we must have $n_j = q_j/2$ and we let $n_{j+1} = (q_{j+1} - 1)/2$. Then

$$A(n,q;Q) = \sum_{j=1}^{J-1} (-1)^{j-1} q_j q_{j+1} \left(\frac{n_j}{q_j} - \frac{n_{j+1}}{q_{j+1}}\right)^2 + \sum_{\substack{1 \leq j \leq J-1 \\ \frac{n_j}{q_j} < \frac{n_{j+1}}{q_{j+1}} < \frac{n_{j+2}}{q_{j+2}}}} (-1)^j + \epsilon \tag{5.2}$$

where ϵ and J are defined as follows: Let J be the smallest integer for which $n_J = 0$ or q_J. If $n_J = 0$ let I be the smallest integer $i \geq 1$ for which $n_i/q_i \leq 1/2$, and then let $\epsilon = 0$ if I is odd, and $\epsilon = 1$ if I is even. If $n_J = q_J$ then let $\epsilon = (-1)^{J-1}$.

We begin our proofs with a technical lemma:

Lemma 5.5. *Let q and Q be coprime integers. If $0 \leq n \leq q-1$ then*

$$A(n,q;Q) = 2\sum_{i=1}^{n}\left[\frac{iQ}{q}\right] - \sum_{i=1}^{2n}\left[\frac{iQ}{q}\right] + \frac{n^2Q}{q} + \begin{cases} 1 & \text{if } n \geq q/2 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For $n=0$ we have $0=0$. Otherwise $1 \leq n \leq q-1$ so that $(iQ)_q < (-nQ)_q$ iff $(iQ)_q + (nQ)_q < q$ iff $\left\{\frac{iQ}{q}\right\} + \left\{\frac{nQ}{q}\right\} < 1$ iff $\left[\frac{(n+i)Q}{q}\right] - \left[\frac{nQ}{q}\right] - \left[\frac{iQ}{q}\right] = 0$ (and this equals 1 otherwise). Also $(iQ)_q = (-nQ)_q$ iff $i = q-n$ which holds in our range iff $n \geq q/2$. Hence

$$\begin{aligned} A(n,q;Q) &= \sum_{i=1}^{n}\left(1 - \left[\frac{(n+i)Q}{q}\right] + \left[\frac{nQ}{q}\right] + \left[\frac{iQ}{q}\right] - \frac{(-nQ)_q}{q}\right) \\ &= \sum_{i=1}^{n}\left(\left[\frac{iQ}{q}\right] - \left[\frac{(n+i)Q}{q}\right] + \frac{nQ}{q}\right) = 2\sum_{i=1}^{n}\left[\frac{iQ}{q}\right] - \sum_{i=1}^{2n}\left[\frac{iQ}{q}\right] + \frac{n^2Q}{q} \end{aligned}$$

plus 1 if $n \geq q/2$, since $\left[\frac{nQ}{q}\right] - \frac{(-nQ)_q}{q} = \frac{nQ}{q} - \frac{(nQ)_q + (-nQ)_q}{q} = \frac{nQ}{q} - 1$.

Proof of Theorem 5.1. As $\sum_{j=x+1}^{x+q}\left\{\frac{mj}{q}\right\} = \sum_{i=0}^{q-1}\left\{\frac{i}{q}\right\} = \frac{q-1}{2}$, we have

$$\begin{aligned} &\sum_{j=1}^{2k}\left[\frac{mj}{q}\right] - 2\sum_{j=1}^{k}\left[\frac{mj}{q}\right] - \left[\frac{mk^2}{q}\right] = 2\sum_{j=1}^{k}\left\{\frac{mj}{q}\right\} - \sum_{j=1}^{2k}\left\{\frac{mj}{q}\right\} + \left\{\frac{mk^2}{q}\right\} \\ &= 2\sum_{j=1}^{n}\left\{\frac{mj}{q}\right\} - \sum_{j=1}^{2n}\left\{\frac{mj}{q}\right\} + \left\{\frac{mn^2}{q}\right\} = \sum_{j=1}^{2n}\left[\frac{mj}{q}\right] - 2\sum_{j=1}^{n}\left[\frac{mj}{q}\right] - \left[\frac{mn^2}{q}\right], \end{aligned}$$

and similarly $\left[\frac{2mk}{q}\right] - 2\left[\frac{mk}{q}\right] = \left[\frac{2mn}{q}\right] - 2\left[\frac{mn}{q}\right]$, so that the desired quantity

$$\begin{aligned} \omega_q &= \left[\frac{mk^2}{q}\right] + 2\sum_{j=1}^{k-1}\left[\frac{mj}{q}\right] - \sum_{j=1}^{2k-1}\left[\frac{mj}{q}\right] = \left[\frac{mn^2}{q}\right] + 2\sum_{j=1}^{n-1}\left[\frac{mj}{q}\right] - \sum_{j=1}^{2n-1}\left[\frac{mj}{q}\right] \\ &= A(n,q;m) - \begin{cases} 1 & \text{if } n \geq q/2 \\ 0 & \text{otherwise} \end{cases} - \left\{\frac{mn^2}{q}\right\} + \left[\frac{2mn}{q}\right] - 2\left[\frac{mn}{q}\right] \end{aligned}$$

by Lemma 5.5.

Proof of Proposition 5.2. If $n=0$ then $l=0, N=0$ so we have $0=0$ in (5.1). For $1 \leq n \leq q-1$, let $v = \left[\frac{Qn}{q}\right]$. Then

$$\begin{aligned} \sum_{i=1}^{n}\left[\frac{Qi}{q}\right] &= \sum_{j=0}^{v-1} j\left(\left[\frac{q(j+1)-1}{Q}\right] - \left[\frac{qj-1}{Q}\right]\right) + v\left(n - \left[\frac{qv-1}{Q}\right]\right) \\ &= vn - \sum_{j=1}^{v}\left[\frac{qj-1}{Q}\right] = vn - \sum_{j=1}^{v}\left[\frac{qj}{Q}\right] + \left[\frac{v}{Q}\right], \end{aligned}$$

since $\left[\frac{qj-1}{Q}\right] = \left[\frac{qj}{Q}\right]$ unless $Q|j$. Hence, as $\left[\frac{v}{Q}\right] = \left[\frac{n}{q}\right]$, and as $v = N$ when $l \geq 0$ and $v = N-1$ when $l < 0$, we have

$$\sum_{i=1}^{n}\left[\frac{Qi}{q}\right] + \sum_{j=1}^{N}\left[\frac{qj}{Q}\right] = nN + \left[\frac{n}{q}\right] + \begin{cases} \left[\frac{-l}{Q}\right] & \text{if } l < 0; \\ 0 & \text{if } l \geq 0, \end{cases} \tag{5.3}$$

since $\frac{qN}{Q} - n = \frac{-l}{Q}$. Similarly

$$\sum_{i=1}^{2n}\left[\frac{Qi}{q}\right] + \sum_{j=1}^{2N}\left[\frac{qj}{Q}\right] = 4nN + \left[\frac{2n}{q}\right] + \begin{cases} \left[\frac{-2l}{Q}\right] & \text{if } l < 0; \\ 0 & \text{if } l \geq 0. \end{cases}$$

Therefore the left side of (5.1) equals, using Lemma 5.5,

$$\frac{n^2Q}{q} + \frac{N^2q}{Q} - 2nN = \frac{(nQ)^2 + (Nq)^2 - 2nQNq}{Qq} = \frac{(nQ-Nq)^2}{Qq} = Qq\left|\frac{n}{q} - \frac{N}{Q}\right|^2,$$

plus 1 if $n > q/2$, minus 1 if $l < 0$ and $L < 0$.

Justification of Algorithm 5.4. Let $l_j := q_{j+1}n_j - q_jn_{j+1}$. Then $l_{j+1} \equiv q_{j+2}n_{j+1} \equiv q_jn_{j+1} \equiv -l_j \pmod{q_{j+1}}$ (so that $L_j = L$ in Proposition 5.2 equals l_{j+1}). Now $A(n_j, q_j; q_{j-1}) = A(n_j, q_j; q_{j+1})$ so Proposition 5.2 implies that $A(n_j, q_j; q_{j+1}) + A(n_{j+1}, q_{j+1}; q_{j+2})$ equals

$$\frac{l_j^2}{q_jq_{j+1}} - \begin{cases} 1 & \text{if } l_j, l_{j+1} < 0 \\ 0 & \text{otherwise} \end{cases} + \begin{cases} 1 & \text{if } n_j > q_j/2 \\ 0 & \text{otherwise.} \end{cases} \tag{5.4}$$

Using the identity

$$A(n, q; Q) = \sum_{j=1}^{J-1}(-1)^{j-1}(A(n_j, q_j; q_{j+1}) + A(n_{j+1}, q_{j+1}; q_{j+2})) \ + (-1)^{J-1}A(n_J, q_J; q_{J+1})$$

the first two terms in (5.2) follow from summing the first two terms in (5.4) (as $l_j < 0$ iff $n_j/q_j < n_{j+1}/q_{j+1}$). For the third term note that since n_{j+1}/q_{j+1} is "close" to n_j/q_j, one can easily prove that $n_j/q_j \leq 1/2$ for $I \leq j \leq J$, and in particular $n_J = 0$. Hence if I exists then $\epsilon = \sum_{j=1}^{I-1}(-1)^{j-1} + A(0, q_j; q_{j+1})$ which gives the result since $A(0, q; Q) = 0$. If I does not exist then $n_j = q_j$ and the result follows since $A(q, q; Q) = 1$.

5.2. Generalized reciprocity law. We can significantly generalize Proposition 5.2 using the same proof, suitably modified, with the following definition: Let

$$A(n, m, q; Q) := \#\{i,\ 1 \leq i \leq n :\ (iQ)_q \leq (-mQ)_q\} - \frac{n(-mQ)_q}{q}.$$

For any integers $0 \leq m, n \leq q$ we have

$$A(n, m, q; Q) = \sum_{i=1}^{n}\left[\frac{iQ}{q}\right] + \sum_{i=1}^{m}\left[\frac{iQ}{q}\right] - \sum_{i=1}^{n+m}\left[\frac{iQ}{q}\right] + \frac{mnQ}{q},$$

plus 1 if $n = q$; hence $A(n, m, q; Q) = A(m, n, q; Q)$. As above, let N be the nearest integer to Qn/q, and M be the nearest integer to Qm/q. Then

$$A(n, m, q; Q) + A(N, M, Q; q) = qQ\left(\frac{m}{q} - \frac{M}{Q}\right)\left(\frac{n}{q} - \frac{N}{Q}\right) = \frac{l_m l_n}{qQ},$$

plus $\left[\frac{|l_n|}{Q}\right]$ if $l_n < 0$, plus $\left[\frac{|l_m|}{Q}\right]$ if $l_m < 0$, minus $\left[\frac{|l_m+l_n|}{Q}\right]$ if $l_m + l_n < 0$, plus 1 if $M + N \geq Q$ and $M \neq Q$, or if $M = N = Q$. This may be rephrased as follows:

If $l_m = 0$ or $l_n = 0$ then $A(n, m, q; Q) + A(N, M, Q; q) = 0$, unless $N = Q$ whence it $= 1$. Otherwise $A(n, m, q; Q) + A(N, M, Q; q) = \frac{l_m^* l_n^*}{qQ} + \eta + [\frac{M+N}{Q}]$ where $0 < l_m^*, l_n^* < q$ and $|\eta| < 1$; specifically

$l_m^* = l_m,\ l_n^* = l_n,\ \eta = 0$ if $l_m, l_n > 0$;

$l_m^* = q - l_m,\ l_n^* = -l_n,\ \eta = -\left\{\frac{qM}{Q}\right\}$ if $l_m + l_n \geq 0 > l_n$;

$l_m^* = l_m,\ l_n^* = q + l_n,\ \eta = \left\{\frac{q(M+N)}{Q}\right\} - \left\{\frac{qN}{Q}\right\}$ if $0 > l_m + l_n > l_n$; and

$l_m^* = -l_m,\ l_n^* = -l_n,\ \eta = -[\frac{(qM)_Q+(qN)_Q}{Q}]$ if $0 > l_m, l_n$.

5.3. Lower bounds on $A(n, q; Q)$. With the notation as above and $q > Q$, we have $A(n, q; Q) \geq -Q$, trivially. This is "best possible" up to the constant since, $A(\frac{q-1}{2}, q; q-1) = -(q-1)^2/4q \sim -Q/4$ for q odd. One can give rather more precise estimates for the small values using the ideas (and notation) of Algorithm 5.4:

Corollary 5.6. *With the notation as above and $q > Q$, we have*

$$\frac{1}{4}\sum_{t\geq 1} r_{2t-1} + J \geq A(n, q; Q) \geq -\frac{1}{4}\sum_{t\geq 1} r_{2t} - J.$$

Select t so that $r_{2t} = \max_{j\geq 1} r_{2j}$. If $r_{2t} \geq 2$ then there exists n such that $-r_{2t}/6 \geq A(n, q; Q) \geq -(r_{2t} + 5)/4$. In particular if $Q > 2(q)_Q$ then there exists n such that $A(n, q; Q) \leq -Q/6(q)_Q$.

Proof. Each term in the first sum in (5.2) has size $\leq (q_j/2)^2/(q_j q_{j+1}) = q_j/4q_{j+1} \leq (r_j + 1)/4$, and the other terms sum up to no more than $J/2 + 1$. This yields bounds.

Given q and Q, one has the sequence $q_1, q_2, \ldots, q_K = 1$ as in Algorithm 5.4. We will construct our value of n by specifying $l_{K-1}, l_{K-2}, \ldots, l_1$, since then $n_j = (q_j n_{j+1} + l_j)/q_{j+1}$ for each j, and $\frac{n}{q} = \sum_{j=1}^{K-1} \frac{l_j}{q_j q_{j+1}}$. Any such sequence $\{l_j\}_{j\geq 1}$ leads to a valid sequence $\{n_j\}_{j\geq 1}$ provided $l_j \equiv -l_{j+1} \pmod{q_{j+1}}$ and $-q_j/2 < l_j \leq q_j/2$ for each j.

Select t for which q_{2t}/q_{2t+1} is maximal. Let b be the largest integer such that $bq_{2t+1} - 1 \leq q_{2t}/2$: note that $b \geq 1$ if and only if $q_{2t}/q_{2t+1} > 2$. We select $l_j = (-1)^j(bq_{2t+1} - 1)$ for all

$j \leq 2t$, and $l_j = (-1)^{j+1}$ for all $K-1 \geq j \geq 2t+1$, except if $q_{K-1} = 2$ and K is odd in which case $l_{K-1} = 1$. Note that at least one of l_j and l_{j+1} is positive for each j. Also $n_J = q_J$ (and $J = K-1$) iff $q_{K-1} = 2$; otherwise $I = 1$ so that $\epsilon = 0$. Hence, by (5.2),

$$A(n,q;Q) = (bq_{2t+1} - 1)^2 \sum_{j=1}^{2t} \frac{(-1)^{j-1}}{q_j q_{j+1}} + \sum_{j=2t+1}^{J-1} \frac{(-1)^{j-1}}{q_j q_{j+1}} + \epsilon$$

where $\epsilon = (-1)^K$ if $q_{K-1} = 2$, and $\epsilon = 0$ otherwise. Now since these are alternating sums with increasing terms, each is majorized by the final term. Hence the final two terms together have absolute value ≤ 1, and $\frac{1}{q_{2t-1}q_{2t}} - \frac{1}{q_{2t}q_{2t+1}} \geq \sum_{j=1}^{2t} \frac{(-1)^{j-1}}{q_j q_{j+1}} \geq -\frac{1}{q_{2t}q_{2t+1}}$. Now $q_{2t-1} = r_{2t-1}q_{2t} + q_{2t+1} \geq q_{2t} + q_{2t+1}$, so that $\frac{1}{q_{2t-1}q_{2t}} - \frac{1}{q_{2t}q_{2t+1}} \leq -\frac{1}{(q_{2t}+q_{2t+1})q_{2t+1}}$. Therefore if $q_{2t} \geq 2q_{2t+1} - 2$ (so that $b \geq 1$) then

$$-\frac{q_{2t}}{6q_{2t+1}} \geq -\frac{b^2}{(2b+2)(2b+3)} \cdot \frac{q_{2t}}{q_{2t+1}} \geq A(n,q;Q) \geq -\frac{q_{2t}}{4q_{2t+1}} - 1.$$

Note that if $q_{2t} < 2q_{2t+1} - 2$ then $r_{2t} = 1$.

6. Lower bounds.

Define $A^*(n,q;Q) = 0$ if $n = 0$, and

$$A^*(n,q;Q) := \#\{i,\ 1 \leq i \leq n-1 :\ (iQ)_q \leq (-nQ)_q\} - \frac{n(-nQ)_q}{q}$$

if $n \geq 1$. Note that $A^*(n,q;Q) = A(n,q;Q)$, minus 1 if $l \geq 0$. Moreover $A(n,q;Q) \leq n$ whereas $A^*(n,q;Q) \leq n-1$.

Proof of Theorem 2$_{\text{even}}$. By Corollary 5.3, we have, when $(m,q) = 1$,

$$\omega_q\left((mk^2)!P(2m,2mk)\right) = \frac{l^2}{qm} - A(N,m;q) - \left\{\frac{mn^2}{q}\right\} + \begin{cases} 1 & \text{if } l < 0 \leq L \\ 0 & \text{otherwise.} \end{cases}$$

This can be negative; for example if $(q)_m \leq m/2$ and $m < \sqrt{q}$ then let $n = 1 + [q/m]$ so that $l = m - (q)_m$, $L = (q)_m$, $N = 1$ and the sum is $\frac{(m-(q)_m)^2}{qm} - \frac{(q)_m}{m} - \{\frac{l^2-q^2}{qm}\} \leq \frac{m^2}{qm} - \frac{1}{m} - 0 < 0$. Indeed if q is prime with $q \equiv 1 \pmod m$ and $q > m^2$ then this implies that $v_q\left((mn^2)!P(2m,2mn)\right) < 0$. To compensate for this we are forced to multiply $(mk^2)!P(2m,2mk)$ through by something like $(mk)!/k!^m$ or some larger multiple of k, to obtain an integer because, in our example, $[\frac{(m-1)n}{q}] = 0$ while $[\frac{mn}{q}] = 1$. Now $\omega_q\left(\frac{(mk)!}{k!^m}\right) = N$, minus 1 if $l < 0$. Hence $\omega_q\left((mk^2)! \cdot \frac{(mk)!}{k!^m} \cdot P(2m,2mk)\right)$

$$= N - 1 - A^*(N,m;q) + \frac{l^2}{qm} - \left\{\frac{mn^2}{q}\right\} + \begin{cases} 1 & \text{if } L < 0 \leq l \\ 0 & \text{otherwise.} \end{cases} \geq \frac{l^2}{qm} - \left\{\frac{mn^2}{q}\right\} > -1,$$

and so is ≥ 0 as ω_q is an integer.

If $(q, m) = g > 1$ let $q = Qg,\ m = Mg$ so that $(Q, M) = 1$. Then, since $\sum_{j=0}^{q-1}\{jm/q\} = q(Q-1)/2$ we have

$$\begin{aligned}\omega_q &= \left[\frac{mk^2}{q}\right] + \left[\frac{mk}{q}\right] - m\left[\frac{k}{q}\right] + \sum_{j=0}^{k-1}\left(\left[\frac{mj}{q}\right] - \left[\frac{m(k+j)}{q}\right]\right)\\ &= \left[\frac{mn^2}{q}\right] + \left[\frac{mn}{q}\right] - m\left[\frac{n}{q}\right] + \sum_{j=0}^{n-1}\left(\left[\frac{mj}{q}\right] - \left[\frac{m(n+j)}{q}\right]\right)\\ &= \left[\frac{Mn^2}{Q}\right] + \left[\frac{Mn}{Q}\right] + \sum_{j=0}^{n-1}\left(\left[\frac{Mj}{Q}\right] - \left[\frac{M(n+j)}{Q}\right]\right)\\ &= \omega_Q\left((Mn^2)!(Mn)! \cdot P(2M, 2Mn)\right) \geq M\left[\frac{n}{Q}\right] \geq 0\end{aligned}$$

using the result established above with (n, M, Q) in place of (k, m, q).

Proof of Theorem 2$_{\text{odd}}$. We deal with the general case by replacing r by $R := r/(r, q)$, and q by $Q := q/(r, q)$ so that $\omega_q((2rk^2)!P(r, 2rk)/2^{2rk^2}) = \omega_Q((2Rn^2)!P(R, 2Rn)/2^{2Rn^2})$ where $n = (k)_q$, and noting that $\omega_q\left(\frac{(rk)!}{k!^r} \cdot \left(\frac{(2rk)!}{k!^{2r}}\right)^2\right) = \omega_Q\left(\frac{(Rn)!}{n!^R} \cdot \left(\frac{(2Rn)!}{n!^{2R}}\right)^2\right) + 5R[\frac{n}{Q}]$.

Henceforth we work in the case that $(r, q) = 1$: By (4.3) we have that

$$\omega_q(P(r, 2rk)/2^{2rk^2}) = \omega_q\left(\frac{P(2r, 2rk)^2 P(2r, 4rk)}{P(4r, 4rk)}\right) - \omega_{2q}(P(2r, 4rk)).$$

Therefore, by Corollary 5.3, we deduce that $\frac{2rk^2}{q} + \omega_q(P(r, 2rk)/2^{2rk^2})$ equals

$$2 \cdot \frac{l_1^2}{qr} + \frac{l_2^2}{qr} - \frac{l_2^2}{q \cdot 2r} - \frac{(2l_1)^2}{2q \cdot r} = \frac{l_2^2}{2qr} \tag{6.1}$$

where l_1, l_2 are the least residues, in absolute value, of $kr, 2kr \pmod q$, respectively, plus

$$A(N_1, r; 2q) + A(N_2, 2r; q) - A^*(N_2 - r[2n/q], r; q) - 2A^*(N_1, r; q) \tag{6.2}$$

where $N_1 = (rn - l_1)/q$ and $N_2 = 2N_1$ minus 1 if $l \leq -q/4$, plus 1 if $l > q/4$ (and note that $l_2 = 2l_1 + q(2N_1 - N_2)$), plus an integer between 0 and 5. To see this last remark note that in (6.2) the terms "$+A$" have $+1$ if $l < 0 \leq L$, and the terms with "$-A^*$" have $+1$ if $l, L < 0$, since $(NQ)_m \leq (-NQ)_m$ iff $L \geq 0$.

We want a lower bound on the quantity in (6.2), which is the sum of two components. First the count of elements of certain sets: if $N_1 \geq 1$ then $-\#\{i,\ 1 \leq i \leq N_1 - 1 :\ (iq)_r \leq (-N_1 q)_r\} \geq -(N_1 - 1) \geq -[\frac{rn}{q}]$ since $N_j = [\frac{jrn}{q}]$, plus 1 if $l_j < 0$, so that $N_j - 1 \leq [\frac{jrn}{q}]$. If $N_1 = 0$ then we go back to the original form since $l_1 \geq 0$, and $-\#\{i,\ 1 \leq i \leq 0:\ (iq)_r \leq 0\} = 0 = -N_1 = -[\frac{rn}{q}]$. Similar arguments hold when $N_2 > r[2n/q]$, and if $N_2 = r[2n/q]$ since $l_2 \geq 0$, so we get the lower bound $r[2n/q] - [\frac{2rn}{q}]$ for the relevant set. Therefore in total we have

$$\geq -\left[\frac{2rn}{q}\right] - 2\left[\frac{rn}{q}\right] + r\left[\frac{2n}{q}\right].$$

The second components in the definition of A and A^* contribute to (6.2):

$$-\frac{N_1(-2N_1q)_r}{r} - \frac{N_2(-N_2q)_{2r}}{2r} + \frac{(N_2 - r[2n/q])(-N_2q)_r}{r} + 2\frac{N_1(-N_1q)_r}{r},$$

so in total (6.2) is $\geq -\left[\frac{2rn}{q}\right] - 2\left[\frac{rn}{q}\right]$

$$+\begin{cases} N_1 & \text{if } L_1 > 0 \\ 0 & \text{otherwise} \end{cases} \quad -\frac{L_2N_2}{2r} + \begin{cases} L_2 & \text{if } n \geq q/2 \text{ and } L_2 > 0 \\ L_2 + r & \text{if } n \geq q/2 \text{ and } L_2 \leq 0 \\ 0 & \text{otherwise} \end{cases} \tag{6.3}$$

where L_1, L_2 are the least residues, in absolute value of $N_1q \pmod r), N_2q \pmod{2r}$, respectively. Note that $|L_2| \leq r$. If $n \geq q/2$ then $N_2 \geq r$, so if $L_2 \leq 0$ then (6.3) is $\geq L_2(1 - N_2/2r) + r \geq r + L_2/2 \geq r/2$, and if $L_2 > 0$ then (6.3) is $\geq L_2(1 - N_2/2r) \geq 0$. If $n < q/2$ then $N_2 \leq r$ and (6.3) is $-\frac{L_2N_2}{2r}$. If $L_2 \leq r - 1$ then this is $\geq -\frac{(r-1)N_2}{2r} \geq -\frac{N_2-1}{2} \geq -\frac{1}{2}\left[\frac{2rn}{q}\right]$. Finally if $L_2 = r$ then $l_2 = r \geq 0$ so (6.3) is $-\frac{N_2}{2} = -\frac{1}{2}\left[\frac{2rn}{q}\right]$

Hence

$$\left[\frac{2rk^2}{q}\right] + \omega_q(P(r, 2rk)/2^{2rk^2}) + \frac{3}{2}\cdot\left[\frac{2rn}{q}\right] + 2\left[\frac{rn}{q}\right] \geq \frac{l_2^2}{2qr} - \left\{\frac{2rk^2}{q}\right\} \tag{6.4}$$

which is an integer > -1 and so ≥ 0. Now $\left[\frac{rn}{q}\right] \leq \frac{1}{2}\cdot\left[\frac{2rn}{q}\right]$ and so

$$(2rk^2)!\ \frac{(2rk)!^2(rk)!}{k!^{5r}}\ \frac{P(r, 2rk)}{2^{2rk^2}}$$

is an integer.

Acknowledgments: The author would like to thank Professors Andrew Granville and Jon Keating for their advice and suggestions.

References.

1. J. Brian Conrey and David W. Farmer, *Mean values of L-functions and symmetry*, Internat. Math. Res. Notices **17** (2000), 883–908.

2. J. Brian Conrey, David W. Farmer, Jon P. Keating, Michael O. Rubinstein and Nina C. Snaith, *Integral moments of L-functions*, Proc. London Math. Soc. **91** (2005), 33–104.

3. J. Brian Conrey and Amit Ghosh, *On mean values of the zeta function*, Mathematika **31** (1984), 159–161.

4. Andrew Granville, *Arithmetic Properties of Binomial Coefficients I: Binomial coefficients modulo prime powers*, Canadian Mathematical Society Conference Proceedings **20** (1997), 253-275.

5. Nicholas M. Katz and Peter Sarnak, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. **36** (1999), 126.

6. Jon Keating and Nina Snaith, *Random matrix theory and* $\zeta(1/2+it)$, Comm. Math. Phys. **214** (2000), 5789.

7. K. Ramachandra, *Some remarks on the mean-value of the Riemann zeta-function and other Dirichlet series, II*, Hardy-Ramanujan J **3** (1980), 1-25.

8. Zeev Rudnick and K. Soundararajan, *Lower bounds for moments of L-functions*, Proc. Natl. Acad. Sci. USA **102** (2005), 6837–6838.

9. Zeev Rudnick and K. Soundararajan, *Lower bounds for moments of L-functions: symplectic and orthogonal examples*, Multiple Dirichlet series, automorphic forms, and analytic number theory, Proc. Sympos. Pure Math. **75**, Amer. Math. Soc, Providence, RI, 2006, pp. 293–303.

10. K. Soundararajan, *Moments of the Riemann zeta-function*, Annals of Math (to appear).