Prime Power Divisors of the Number of $n \times n$ Alternating Sign Matrices

Darrin D. Frey
Department of Science and Math
Cedarville University
Cedarville, OH 45314
freyd@cedarville.edu

and

James A. Sellers
Department of Mathematics
The Pennsylvania State University
University Park, PA 16802
sellersj@math.psu.edu

January 15, 2002

Abstract

We let $A(n)$ equal the number of $n \times n$ alternating sign matrices. From the work of a variety of sources, we know that

$$A(n) = \prod_{\ell=0}^{n-1} \frac{(3\ell+1)!}{(n+\ell)!}.$$

We find an efficient method of determining $ord_p(A(n))$, the highest power of p which divides $A(n)$, for a given prime p and positive integer n, which allows us to efficiently compute the prime factorization of $A(n)$. We then use our method to show that for any nonnegative integer k, and for any prime $p > 3$, there are infinitely many positive integers n such that $ord_p(A(n)) = k$. We show a similar but weaker theorem for the prime $p = 3$, and note that the opposite is true for $p = 2$.

1 Background

An $n \times n$ **alternating sign matrix** is an $n \times n$ matrix consisting entirely of 1s, 0s, and -1s with the property that the sum of the entries of each row and each column must be 1 and the signs of the nonzero entries in each row and column must alternate. For example, the matrix

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

is one of the 42 4×4 alternating sign matrices.

Let $A(n)$ denote the number of $n \times n$ alternating sign matrices. Because each permutation matrix is also an alternating sign matrix, it is clear that $A(n) \geq n!$.

Recently, Zeilberger [9] proved that

$$A(n) = \prod_{\ell=0}^{n-1} \frac{(3\ell+1)!}{(n+\ell)!}. \tag{1}$$

The reader interested in the development of (1) is encouraged to see the survey articles of Robbins [8] and Bressoud and Propp [4], as well as the award–winning text of Bressoud [2].

In [5], we gave a characterization of the values of n for which $A(n)$ is odd. In this paper, we give a method for determining $ord_p(A(n))$, the highest power of a given prime p that divides $A(n)$ for given n. As a consequence we obtain a fast method for calculating $A(n)$ for large n. (In general, $A(n)$ is difficult to compute using (1) if n is large.) Our main theorem however, is Theorem 1.1 which comes as a consequence of our method. Theorem 1.1 is an interesting contrast to the situation when $p = 2$ where the opposite is true (see [6, Corollary 3.8]). We also give a characterization of when a given prime divides $A(n)$ based on its base p representation.

The basic machinery is given in Section 2 and was largely developed in [5], (where the authors were primarily interested in the parity of $A(n)$), but is greatly simplified and generalized here. As this paper was in preparation for publication, we were contacted by Cartwright and Kupka and made aware of their paper [3] which essentially duplicates our method for determining $ord_p(A(n))$. However, we include that result here anyway as our proof emphasizes the periodicity of the function $c_{p,k}(n)$ which is used in the proof of Theorem 1.1 and is somewhat shorter and easier (though Cartwright and Kupka's perspective is broader than ours).

Theorem 1.1. *If p is a prime greater than 3, then for each nonnegative integer k there exist infinitely many positive integers n for which $ord_p(A(n)) = k$.*

2 Calculation of $A(n)$

We begin by stating the following lemma which is critical to our discussion. For a proof of this lemma, see [7, Theorem 2.29].

Lemma 2.1. *For any prime p and any positive integer N,*

$$ord_p(N!) = \sum_{k\geq 1} \left\lfloor \frac{N}{p^k} \right\rfloor .$$

Applying Lemma 2.1 to (1) then gives us

$$ord_p(A(n)) = \sum_{\ell=0}^{n-1}\sum_{k\geq 1} \left\lfloor \frac{3\ell+1}{p^k} \right\rfloor - \sum_{\ell=0}^{n-1}\sum_{k\geq 1} \left\lfloor \frac{n+\ell}{p^k} \right\rfloor = \sum_{k\geq 1} c_{p,k}(n), \tag{2}$$

where

$$c_{p,k}(n) := \sum_{\ell=0}^{n-1} \left(\left\lfloor \frac{3\ell+1}{p^k} \right\rfloor + \left\lfloor \frac{\ell}{p^k} \right\rfloor \right) - \sum_{\ell=0}^{2n-1} \left\lfloor \frac{\ell}{p^k} \right\rfloor . \tag{3}$$

$\left(\text{Note that } \sum_{\ell=0}^{n-1} \left\lfloor \frac{n+\ell}{p^k} \right\rfloor = \sum_{\ell=0}^{2n-1} \left\lfloor \frac{\ell}{p^k} \right\rfloor - \sum_{\ell=0}^{n-1} \left\lfloor \frac{\ell}{p^k} \right\rfloor . \right)$

We introduce the increment

$$c_{p,k}(n+1) - c_{p,k}(n) = \left\lfloor \frac{3n+1}{p^k} \right\rfloor + \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{2n+1}{p^k} \right\rfloor - \left\lfloor \frac{2n}{p^k} \right\rfloor$$

of $c_{p,k}(n)$ and note that the increment is periodic of period p^k as Proposition 2.2 shows.

Proposition 2.2. *Let k, n be positive integers and p be prime. Then*

$$c_{p,k}(p^k + n + 1) - c_{p,k}(p^k + n) = c_{p,k}(n+1) - c_{p,k}(n).$$

Proof.

$$
\begin{aligned}
& c_{p,k}(p^k+n+1) - c_{p,k}(p^k+n) \\
= & \left\lfloor \frac{3(p^k+n)+1}{p^k} \right\rfloor + \left\lfloor \frac{p^k+n}{p^k} \right\rfloor - \left\lfloor \frac{2p^k+2n+1}{p^k} \right\rfloor - \left\lfloor \frac{2p^k+2n}{p^k} \right\rfloor \\
= & \left\lfloor 3 + \frac{3n+1}{p^k} \right\rfloor + \left\lfloor 1 + \frac{n}{p^k} \right\rfloor - \left\lfloor 2 + \frac{2n+1}{p^k} \right\rfloor - \left\lfloor 2 + \frac{2n}{p^k} \right\rfloor \\
= & \left\lfloor \frac{3n+1}{p^k} \right\rfloor + \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{2n+1}{p^k} \right\rfloor - \left\lfloor \frac{2n}{p^k} \right\rfloor + 3 + 1 - 2 - 2 \\
= & c_{p,k}(n+1) - c_{p,k}(n).
\end{aligned}
$$

□

If $p > 2$ and $0 \le n < p^k$, we can easily see that

$$
c_{p,k}(n+1) - c_{p,k}(n) = \begin{cases} 0 & \text{if} \quad 0 \le n < \left\| \frac{p^k}{3} \right\|, n = \left\lfloor \frac{p^k}{2} \right\rfloor, \text{ or } \left\| \frac{2p^k}{3} \right\| \le n < p^k \\ 1 & \text{if} \quad \left\| \frac{p^k}{3} \right\| \le n < \frac{p^k}{2} \\ -1 & \text{if} \quad \frac{p^k}{2} < n < \left\| \frac{2p^k}{3} \right\| \end{cases} \tag{4}
$$

where $\|t\|$ is the integer nearest to t. Hence, since the number of $+1$ increments is equal to the number of -1 increments, $c_{p,k}(p^k) = 0$ which means that $c_{p,k}(n)$ is itself periodic of period p^k. If $p = 2$, then equation (4) is nearly the same except that the increment at $\frac{p^k}{2}$ is -1 rather than 0.

Theorem 2.3. *If* $0 \le n < p^k$. *Then*

$$
c_{p,k}(n) = max\left\{0, \frac{p^k}{2} - \left\| \frac{p^k}{3} \right\| - \left| n - \frac{p^k}{2} \right| \right\}.
$$

Consequently, $c_{p,k}(n) = c_{p,k}(p^k - n)$.

Proof. The increment of $c_{p,k}(n)$ in (4) tells us that if $p > 2$, the maximum value of $c_{p,k}(n)$ is $\frac{p^k}{2} - \left\| \frac{p^k}{3} \right\| - \frac{1}{2}$ $\left(\text{when } n = \frac{p^k}{2} \pm \frac{1}{2}\right)$ and that it decrements by 1 moving away from these values in either direction. $\left(\text{If } p = 2, \text{ the maximum value is } \frac{p^k}{2} - \left\| \frac{p^k}{3} \right\| \text{ at } n = \frac{p^k}{2}.\right)$ Note that $\left\| \frac{2p^k}{3} \right\| - \frac{p^k}{2} = \frac{p^k}{2} - \left\| \frac{p^k}{3} \right\|$ so we have complete symmetry about $\frac{p^k}{2}$. If n is within $\left\| \frac{p^k}{3} \right\|$ of $\frac{p^k}{2}$ then we see that $c_{p,k}(n)$ is the difference of this maximum value

$\left(\text{plus } \frac{1}{2} \text{ if } p \neq 2\right)$, and the distance between n and $\frac{p^k}{2}$. If not, then we have passed into an interval where both the value of $c_{p,k}(n)$ and the increment is 0. Thus, we have our result. □

3 Infiniteness Results

In this section, we will prove Theorem 1.1. We first mention two propositions whose proofs we omit since they are straightforward computations.

Proposition 3.1. *If p is a prime and $p \equiv 1 \pmod 6$ then*

$$\begin{aligned} \left\|\frac{p^k}{3}\right\| &= \left\|\frac{p^{k-i}}{3}\right\| + \left\|\frac{p^i}{3}\right\| \cdot p^{k-i} \quad \textit{and} \\ \left\|\frac{2p^k}{3}\right\| &= \left\|\frac{2p^{k-i}}{3}\right\| + \left(\left\|\frac{2p^i}{3}\right\| - 1\right) \cdot p^{k-i}. \end{aligned}$$

Proposition 3.2. *If p is a prime and $p \equiv 5 \pmod 6$, then*

$$\begin{aligned} \left\|\frac{p^k}{3}\right\| &= \left\|\frac{p^{k-2i}}{3}\right\| + \left\|\frac{p^{2i}}{3}\right\| \cdot p^{k-2i}, \\ \left\|\frac{2p^k}{3}\right\| &= \left\|\frac{2p^{k-2i}}{3}\right\| + \left(\left\|\frac{2p^{2i}}{3}\right\| - 1\right) p^{k-2i}, \\ \left\|\frac{p^k}{3}\right\| &= \left\|\frac{2p^{k-2i-1}}{3}\right\| + \left(\left\|\frac{p^{2i+1}}{3}\right\| - 1\right) p^{k-2i-1}, \quad \textit{and} \\ \left\|\frac{2p^k}{3}\right\| &= \left\|\frac{p^{k-2i-1}}{3}\right\| + \left\|\frac{2p^{2i+1}}{3}\right\| \cdot p^{k-2i-1}. \end{aligned}$$

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. If $k = 0$, then we know that $c_{p,i}(p^j) = 0$ for all positive j, so we have established that $ord_p(A(n)) = 0$ for infinitely many positive integers n. Assume then that $k > 0$.

If $p \equiv 1 \pmod 6$, consider $n = \left\|\frac{p^k}{3}\right\| + 1$. Then $n = \left(\left\|\frac{p^{k-i}}{3}\right\| + 1\right) + \left\|\frac{p^i}{3}\right\| \cdot p^{k-i}$ for $0 \leq i \leq k-1$, so by the periodicity of $c_{p,i}$ for each i, we know that $c_{p,k-i}(n) = c_{p,k-i}\left(\left\|\frac{p^{k-i}}{3}\right\| + 1\right) = 1$ for $0 \leq i \leq k-1$. Moreover, since $n < \left\|\frac{p^j}{3}\right\|$ for all $j > k$, $c_{p,j}(n) = 0$ for all $j > k$. Hence, $ord_p(A(n)) = k$.

If $p \equiv 5 \pmod 6$, consider $n = \left\| \frac{p^{2k}}{3} \right\| + 1$. Then $n = \left\| \frac{p^{2k-2i}}{3} \right\| + 1 + \left\| \frac{p^{2i}}{3} \right\| \cdot p^{2k-2i}$ for $0 \leq i \leq k-1$, so by the periodicity of $c_{p,i}$ for each i, we know that $c_{p,2k-2i}(n) = c_{p,2k-2i}\left(\left\| \frac{p^{2k-2i}}{3} \right\| + 1\right) = 1$ for $0 \leq i \leq k-1$. Also, $n = \left\| \frac{p^{2k}}{3} \right\| + 1 = \left\| \frac{2p^{2k-2i-1}}{3} \right\| + 1 + \left(\left\| \frac{2p^{2i+1}}{3} \right\| - 1\right) p^{2k-2i-1}$, so $c_{p,2k-2i-1}(n) = c_{p,2k-2i-1}\left(\left\| \frac{2p^{2k-2i-1}}{3} \right\| + 1\right) = 0$ for $0 \leq i \leq k-1$. Moreover, since $n < \left\| \frac{p^j}{3} \right\|$ for all $j > k$, $c_{p,j}(n) = 0$ for all $j > k$. Hence, $ord_p(A(n)) = k$.

In both cases, for each positive integer k we have established the existence of at least one positive integer n such that $ord_p(A(n)) = k$. To get infinitely many, consider $n+p^j$ where $j > k$. Then since $n \bmod p^i = n < \left\| \frac{p^i}{3} \right\|$ for $k+1 \leq i \leq j$ and $n + p^j < \left\| \frac{p^i}{3} \right\|$ for $i > j$, $c_{p,i}(n+p^j) = c_{p,i}(n)$ for all positive i. Hence, we have $ord_p(A(n+p^j)) = k$ for $j > k$. $\square$

We can prove a result similar to Theorem 1.1 for $p = 3$, although it is somewhat weaker. By considering integers of the form $3^j + 3^k$, where $j > k$, we can show that there are infinitely many positive integers n such that $3^{3^k} | A(n)$. Moreover, by considering integers of the form $3^j + 3^{k-1}$, where $j > k$, we can show that there are infinitely many positive integers n such that $3^{3^k} \not| A(n)$, but $3^{3^{k-1}} | A(n)$. In fact, for a given k, if one can show that there is some integer n such that $ord_3(A(n)) = k$, then there are infinitely many integers m such that $ord_3(A(m)) = k$, namely, the integers $m = 2 \cdot 3^j + n$ where $j > \log_3(n) + 1$. The situation is very different when $p = 2$. In fact, for any positive integer k, there are only finitely many positive integers n for which $ord_2(A(n)) = k$. For a proof of this claim, see [6, Corollary 3.8].

We close this section by noting that the intuition we used to prove Theorem 1.1 and Propositions 3.1 and 3.2 came from viewing Theorem 2.3 in base p. First, $n \bmod p^k$ is simply the last k digits of the base p representation of n. Moreover, in base $p > 2$, $\left\| \frac{p^k}{3} \right\|$ and $\left\| \frac{2p^k}{3} \right\|$ are k-digit numbers of a very special form. For example, for $p = 13$ (which is congruent to 1 mod 6), $\left\| \frac{p^k}{3} \right\| = 444 \cdots 44_{13}$ while $\left\| \frac{2p^k}{3} \right\| = 888 \cdots 89_{13}$, and for $p = 11$ (which is congruent to 5 mod 6), we have $\left\| \frac{p^k}{3} \right\| = 3737 \cdots 37_{11}$ or $3737 \cdots 374_{11}$ and $\left\| \frac{2p^k}{3} \right\| = 7373 \cdots 74_{11}$ or $7373 \cdots 37_{11}$ depending on whether k is even or odd. In general, the digits corresponding to primes $p \equiv 1 \pmod 6$ are $\left\|\frac{p}{3}\right\|$, $\left\|\frac{2p}{3}\right\|$ and $\left\|\frac{2p}{3}\right\|-1$, while the digits corresponding to primes $p \equiv 5 \pmod 6$ are $\left\|\frac{p}{3}\right\|$, $\left\|\frac{2p}{3}\right\|$ and $\left\|\frac{p}{3}\right\| - 1$. If $p = 3$, $\left\|\frac{p^k}{3}\right\|$ is a power of three while $\left\|\frac{2p^k}{3}\right\|$ is twice a power of three (unless $k = 1$). One can use such information to write down a characterization of when $A(n)$ is relatively prime to a given prime p. We do so below. See [3] for a different characterization.

Let the base p representation of a given positive integer n be represented by $n = p^m d_m + p^{m-1} d_{m-1} + \cdots + p d_1 + d_0$ where $0 \le d_i < p$ for $i = 0, \ldots, m$.

Definition 3.3. *Let n be a positive integer, and p any prime greater than 3. Let m be 1 or -1 as $p \equiv 1$ or $-1 \pmod 6$. Consider a sequence of consecutive digits $d_i, d_{i-1}, \ldots, d_{i-j}$ in the base p representation of n. We call such a sequence a* determining sequence *if*

$$\left\|\frac{p^{j+1}}{3}\right\| < p^j d_i + p^{j-1} d_{i-1} + \cdots + d_{i-j} < \left\|\frac{2p^{j+1}}{3}\right\| - \frac{1 + m^{j+1}}{2}.$$

Proposition 3.4. *Using the notation above, the following characterizes for which values of n, $(A(n), p) > 1$.*

- *If $p = 2$, see [5] and [3].*
- *If $p = 3$, $(A(n), 3) = 1$ if and only if whenever $d_i = 1$, $d_j = 0$ for $j = 0, \ldots, i - 1$.*
- *If $p \equiv 1 \pmod 6$, then $(A(n), p) > 1$ if and only if either there is a determining sequence for n with $j \in \{0, 1\}$ or if $d_0 = \left\|\frac{2p}{3}\right\| - 1$.*
- *If $p \equiv 5 \pmod 6$, then $(A(n), p) > 1$ if and only if either there is a determining sequence for n with $j \in \{0, 1, 2\}$ or if $d_1 = \left\|\frac{2p}{3}\right\|$ and $d_0 = \left\|\frac{p}{3}\right\| - 1$.*

4 Running Time Analysis

We provide here an analysis of the speed of the method that we and Cartwright and Kupka independently developed for calculating $c_{p,k}(n)$. As mentioned in Section 2, it is clear that

$$ord_p(A(n)) = \sum_{k \ge 1} c_{p,k}(n).$$

Since $A(n)$ is smooth for each n and only contains primes $p < 3n$, we can now quickly determine the prime factorization of $A(n)$ for large values of n. As an example, we calculated $A(50000)$. Note that $A(50000) \approx \left(\frac{27}{16}\right)^{50000^2/2}$, so that $A(50000)$ has a base 10 representation with approximately 284,000,000 digits. The prime factorization of $A(50000)$ is

$$2^{11102} \cdot 3^{2848} \cdot 5^{2083} \cdot \ldots \cdot 149969^{10} \cdot 149971^{10} \cdot 149993^{2}.$$

This value would certainly be intractable if calculated using (1). The Maple code used to calculate this result can be obtained from the authors.

Calculation of $A(n)$ via the method we describe here is much faster than calculation using (1). Indeed, since no obvious cancellation scheme appears available in (1), calculation of $A(n)$ via (1) will involve $O(n^2)$ operations. This is because the number of operations needed to compute $n!$ is n, (or $n-1$ if one ignores the multiplication by 1). But this implies that the number of multiplications needed to compute $A(n)$ via (1) is at least

$$0+3+6+9+\ldots+3n-3+(n-1)+n+(n+1)+\ldots+(2n-1)$$

which is $O(n^2)$ since $1+2+3+\ldots+n = n(n+1)/2$. The additional multiplications needed to combine all of the separate factorials into one final number will not contribute to a larger order of magnitude, so that $O(n^2)$ is indeed the number of operations involved.

In contrast, determination of the prime factorization of $A(n)$ via the method in Section 2 involves only $O(n)$ computations. The calculation involves finding $ord_p(A(n))$ for each $p \leq 3n$ (since any prime greater than $3n$ will yield $c_{p,k}(n) = 0$ for all k), and thus we are calculating a double sum. The inner sum, which, in practice, runs from $k = 1$ to $\lceil \log_2(n) \rceil + 1$, requires $O(\log(n))$ computations. The outer sum, which involves all primes p less than $3n$, requires $O\left(\frac{n}{\log(n)}\right)$ computations since, by the Prime Number Theorem [1], if $\pi(x)$ equals the number of primes less than or equal to x, then

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

Thus, our algorithm requires $O(n)$ computations since

$$\log(n) \cdot \frac{n}{\log(n)} = n.$$

References

[1] T. M. Apostol, "Introduction to Analytic Number Theory", Springer-Verlag, 1976.

[2] D. M. Bressoud, "Proofs and Confirmations: The story of the alternating sign matrix conjecture", Cambridge University Press, 1999.

[3] D. I. Cartwright and J. Kupka, When Factorial Quotients are Integers, preprint (submitted to *Gazette of the Australian Mathematics Society*).

[4] D. M. Bressoud and J. Propp, How the Alternating Sign Matrix Conjecture Was Solved, *Notices of the American Mathematical Society*, **46** (6) (1999), 637-646.

[5] D. D. Frey and J. A. Sellers, Jacobsthal Numbers and Alternating Sign Matrices, *Journal of Integer Sequences*, **3** (2000), Article 00.2.3.

[6] D. D. Frey and J. A. Sellers, On Powers of 2 Dividing the Values of Certain Plane Partition Functions, *Journal of Integer Sequences*, **4** (2001), Article 01.1.8.

[7] C. T. Long, "Elementary Introduction to Number Theory", 3rd edition, Waveland Press, Inc., Prospect Heights, IL, 1995.

[8] D. P. Robbins, The Story of $1, 2, 7, 42, 429, 7436, \ldots$, *The Mathematical Intelligencer*, **13** (2) (1991), 12-19.

[9] D. Zeilberger, Proof of the alternating sign matrix conjecture, *Electronic Journal of Combinatorics* **3** (1996), R13.