Directed Studies
Distribution of Element Orders in Finite Groups

Alex Simonyi, under the supervision of: Dr. Zoltán Halasi

December 2025

Introduction

Let G be a finite group. Denote the sum of elements in G by $\psi(G)$ i.e.:

$$\psi(G) = \sum_{g \in G} \mathrm{o}(g)$$

Let's take a look now at a slightly modified version of this, with respect to the symmetric groups:

$$f(n) := \sum_{g \in S_n} \mathrm{o}(g)(-1)^{\pi(g)} = 2\psi(A_n) - \psi(S_n)$$

Where $\pi(g)$ is the parity of g as a permutation. We think that $\lim_{n\to\infty} f(n) = -\infty$, while the ratio of the positive, and negative subsums: $\lim_{n\to\infty} \frac{\psi(A_n)}{\psi(S_n)-\psi(A_n)} = 1$, which of both is yet to be proven. This question driven us towards Landau's function (Edmund Landau 1877-1938) where $g(n)$ denotes, the maximal order an element can have in the symmetric group S_n. Landau's function has been widely studied from an analytic point of view, and the following statement has been proved in 1902 by Edmund Landau, and later by others:

$$\lim_{n\to\infty} \frac{\ln(g(n))}{\sqrt{n \ln(n)}} = 1$$

For us this function is important from a rather number theoretic approach, on which we didn't really find any papers.

Parity of Permutations, and Landau's Function

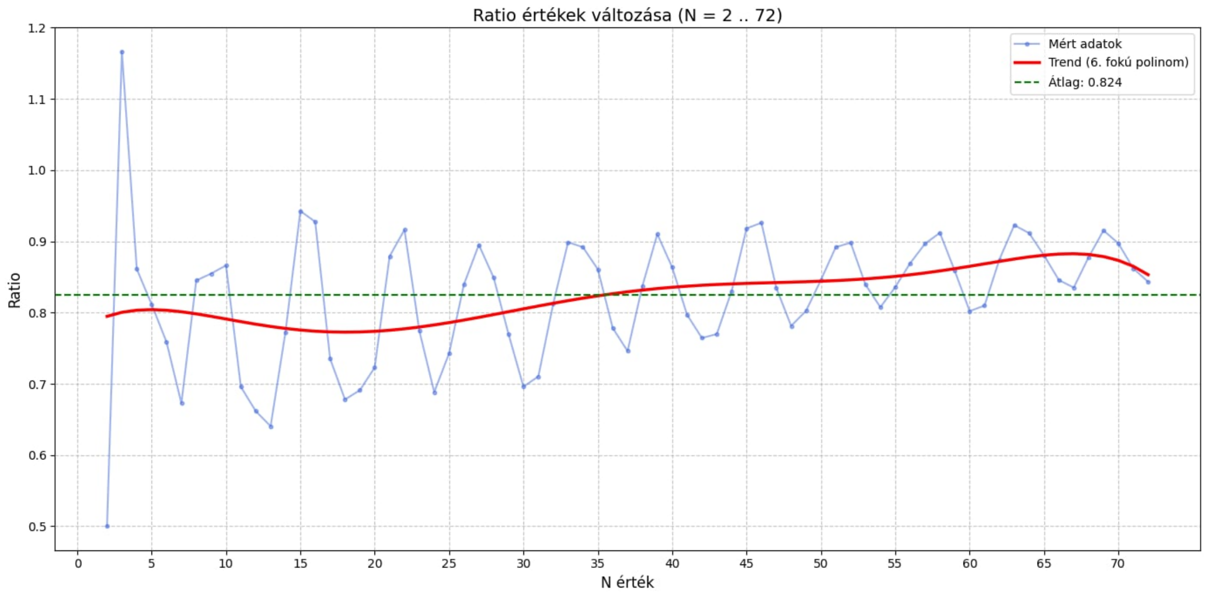
We want to design an element with the greatest order possible in S_n. If we look at the cycle decomposition of a permutation, we find that its order as a group element is the least common multiple, of its cycle lengths. So now we want a set of integers a_i where $\sum a_i = n$, while their least common multiple is as great as possible. Its quite trivial, that we want to use numbers of which any 2 are coprime, furthermore only powers of different primes, since if some a_i isn't a prime power, and is coprime, to any $a_j : j \neq i$, then we can change a_i to a_{i_1} and a_{i_2} where $a_i = a_{i_1} \cdot a_{i_2}$, and since $a_{i_1}, a_{i_2} > 2$ and can't be the same number, $a_{i_1} + a_{i_2} < a_i$. This is what leads to prime numbers, and connection to prime number theorem, which is used in the proof of the theorem regarding the growth of $g(n)$. Lets take a look at when will the permutation with cycle lengths a_i be even, which is exactly if we got an even number of even numbers among a_i. Meaning that we either have no power of 2 or have more than 1 of them (concentrating on the cases, where we have only prime powers), where the second case is making the sum bigger, and does nothing to the least common multiple, which we don't really want, leaving us with slight correspondence between $\prod a_i$ being an even number, and the permutation being odd in the case of a large order. Since it's proved that there are arbitrary long constant sequences in $g(n)$, which means, that if $g(n) = g(n-2)$, then we can construct both even and odd maximal order elements by taking the permutation in S_{n-2} with the order $g(n)$, and on the 2 extra elements do a swap or not. Not only we have odd and even permutations for being of maximal order there are the same number of them. Still the argument about odd permutations being bigger holds for non-maximal elements also, and that's a more general case, which would make $f(n)$ to be negative as $n > 3$, which we checked using python, for small n. Us thinking that $f(n)$ converges to $-\infty$ is mostly based on this. The table below contains the values of $g(n)$, and the corresponding cycle dcompositions up to 20:

n	g(n)	cycle lengths
1	1	1
2	2	2
3	3	3
4	4	4
5	6	2,3
6	6	1,2,3 or 6
7	12	3,4
8	15	3,5
9	20	4,5
10	30	2,3,5

n	g(n)	cycle lengths
11	30	1,2,3,5 or 5,6
12	60	3,4,5
13	60	1,3,4,5
14	84	3,4,7
15	105	3,5,7
16	140	4,5,7
17	210	2,3,5,7
18	210	1,2,3,5,7 or 5,6,7
19	420	3,4,5,7
20	420	1,3,4,5,7

Regarding $g(n)$, based on the arguments in the previous paragraph, we strongly believe, that for $n > 15$ $g(n)$ is even. Using the table on OEIS containing value of $g(n)$ for n up to 65536 we checked, that until then this holds. We think the second limit stated in the introduction is true because of the constant sequences in $g(n)$.

While it is only about the maximal cases, for a general order size, it is probable that as n grows, more and more situations arise where we do not need all the n elements of the set on which the permutation acts for constructing a permutation with that order, making the number of odd, and even permutations of that order equal. The blue points of the graph below are showing the said ratio, seem to be converging, and for some unknown reason fluctuating.



If desired, one can define $f(G)$ notion to any group, by using choosen group's embedding into the symmetric group by how the elements permuting the Cayley table, looking at the imige of said group, which elements now have parity.

References

[1] William Miller, *The Maximum Order of an Element of a Finite Symmetric Group*, American Mathematical Monthly, Volume 94, Issue 6 (Jun. - Jul., 1987), 497-506. .

[2] https://oeis.org/A000793