**Irish Math. Soc. Bulletin**
Number 93, Summer 2024, 39–41
ISSN 0791-5578

# The genesis of a conjecture in number theory

ROBERT HEFFERNAN AND DES MACHALE

ABSTRACT. We discuss how a knowledge of commutativity in finite groups and conjugacy classes in the symmetric group leads to a conjecture in number theory.

Conjectures play an important role in the development of mathematics at all levels and it is sometimes a mystery where they come from. The example to follow convinces us that some conjectures at least come from speculation, experimentation and the invaluable practice of examining as much numerical evidence as you can lay your hands on. First, some background.

If $n$ is a natural number, the (integer) partition function $p(n)$ is the total number of ways of writing $n$ as the sum of natural numbers, without regard to order. For example, since

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1,$$

we have $p(5) = 7$. A great deal is known about the function $p(n)$ but there are still many unanswered questions; for example, we do not know when $p(n)$ is odd or even. Here is a table of values of $p(n)$ for small $n$:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p(n)$ | 1 | 2 | 3 | 5 | 7 | 11 | 15 | 22 | 30 | 42 | 56 | 77 | 101 | 135 | 176 | 231 |

We note that $p(n)$ increases rather quickly; for example $p(50) = 204226$ and $p(100) = 190569292$.

Our aim is to motivate the following conjecture:

**Conjecture 1.** *The values of $n$ for which $p(n)$ divides $n!$ all belong to the finite set*

$$S = \{1,2,3,7,9,10,11,12,14,15,16,17,18,19,20,21,24,28,32,33,39\}.$$

The symmetric group $S_n$ is the group of all permutations on the symbols $\{1,2,3,\cdots,n\}$. $S_n$ has order $n!$ and is a non-commutative group for $n \geq 3$. It is well-known that $S_n$ has exactly $p(n)$ conjugacy classes and since a group $G$ is commutative if and only if it has $|G|$ conjugacy classes, we immediately get

**Theorem 1.** *For $n \geq 3$, $p(n) < n!$.*

This is a crude bound, much weaker than best possible, but a proof involving number theory alone might be quite tricky, and the reader is invited to find one.

In general, if $G$ is a finite group with exactly $k(G)$ conjugacy classes, we form the ratio

$$\Pr(G) = \frac{k(G)}{|G|},$$

---

2020 *Mathematics Subject Classification.* 20A99.
*Key words and phrases.* ipartition function, symmetric group, commuting probability.
Received on 17-1-2024; revised 3-5-2024.
DOI:10.33232/BIMS.0093.39.41.

so that $\Pr(G) = 1$ if and only if $G$ is a commutative group. Note that $\Pr(G)$ is the probability that two elements of the finite group $G$, selected at random with replacement, commute. There is an extensive literature on $\Pr(G)$. (See [2], [5], [3] and [1]). In particular, we have the following results which are of relevance here

**Result 1.** *If $G$ is a non-commutative group, then* $\Pr(G) \leq \frac{5}{8}$.

**Result 2.** *If $H$ is a subgroup of $G$, then* $\Pr(G) \leq \Pr(H)$.

**Result 3.** *If $G$ is an insoluble group, then* $\Pr(G) \leq \frac{1}{12}$.

Applying Result 1 to $S_n$ we get

**Theorem 2.** *For $n \geq 3$, $p(n) \leq \left(\frac{5}{8}\right) n!$.*

Since $S_3$ is a subgroup of $S_n$ for each $n \geq 3$, applying Result 2 we see that, for each $n \geq 3$, $\Pr(S_n) \leq \Pr(S_3) = \frac{1}{2}$. This gives the following improvement on Theorem 2:

**Theorem 3.** *For $n \geq 3$, $p(n) \leq \left(\frac{1}{2}\right) n!$.*

Since, for $n > 1$, $S_{n+1}$ has a subgroup isomorphic to $S_n$, by Result 2 we have $\Pr(S_{n+1}) \leq \Pr(S_n)$, so that

$$\frac{p(n+1)}{(n+1)!} < \frac{p(n)}{n!}.$$

Thus we get

**Theorem 4.** *For $n \geq 2$, $p(n+1) < (n+1)p(n)$.*

Since for $n \geq 5$, $S_n$ is an insoluble group, we have, by Result 3,

**Theorem 5.** *For $n \geq 5$, $p(n) \leq \left(\frac{1}{12}\right) n!$.*

Many other such results are easily deduced. For example we have:

**Theorem 6.** (1) *For $n \geq 4$, $p(n) < \left(\frac{5}{24}\right) n!$.*
(2) *For $n \geq 5$, $p(n) < \left(\frac{7}{20}\right) n!$.*
(3) *For $n \geq t$, $p(n) < \frac{p(t)n!}{t!}$.*

Incidentally, we know of no purely number theoretic solutions to the following pretty problems in number theory, but there are easy solutions using the properties of the symmetric group.

**Problem 1.** *Show that for each $n$, $n!$ can be written as*

$$n! = \sum_{i=1}^{p(n)} c_i,$$

*where $p(n)$ is the partition function and each $c_i$ is a positive integer divisor of $n!$.*

*Solution.* Just take the class equation of $S_n$ which has $p(n)$ conjugacy classes each of whose cardinalities is a divisor of $n!$. Thus $6 = 1+2+3$, $24 = 1+3+6+6+8$, etc. These representations are clearly not unique, since $6 = 2+2+2$ and $24 = 2+4+6+6+6$, etc. $\square$

**Problem 2.** *Show that, for each $n$, $n!$ can be written as*

$$n! = \sum_{i=1}^{p(n)} d_i^2$$

*where $p(n)$ is the partition function and each $d_i$ is a positive integer divisor of $n!$.*

*Solution.* Here we use the degree equation of a group $G$, which states that $|G|$ is the sum of the squares of the degrees of the irreducible complex matrix representations of $G$, which are $k(G)$ in number, i.e.

$$|G| = \sum_{i=1}^{k(G)} d_i^2$$

and each $d_i$ is a divisor of $|G|$. Applying this result to $S_n$ we get

$$n! = \sum_{i=1}^{p(n)} d_i^2$$

as desired. □

Thus $6 = 1^2 + 1^2 + 2^2$, $24 = 1^2 + 1^2 + 2^2 + 3^2 + 3^2$, etc.

And now to our number-theoretic conjecture. Originally, we were trying to prove that for each $t \in \mathbb{N}$ one can find a group $G_t$ with $\Pr(G_t) = \frac{1}{t}$. (Actually, this turns out to be rather easy using direct products of dihedral groups and is left as an exercise for the reader). Looking at $S_n$, we were struck by the number of instances for small $n$ where this phenomenon occurred. The number-theoretic version of this is, of course, "find all $n$ for which $p(n)$ divides $n!$".

One can easily work out the first few values of $n$ for which this happens. They are

$$1, 2, 3, 7, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19, 20, 21, 24, 28, 32, 33, 39, \cdots .$$

This is now sequence A046668 of Sloane's Online Encyclopedia of Integer Sequences [4] but we could not find any more terms greater than 39.

On July 6th, 2018, Vaclav Kotesovec posted the following on [4] after extensive computer calculations: the next term, if it exists, is greater than 2000000.

Hence we are led to formulate Conjecture 1. Currently we do not have a proof of this conjecture but would be pleased to hear from anyone who does.

## References

[1] Robert M. Guralnick and Geoffrey R. Robinson, *On the commuting probability in finite groups*, J. Algebra **300** (2006), no. 2, 509–528.

[2] W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.

[3] Paul Lescot, *Isoclinism classes and commutativity degrees of finite groups*, J. Algebra **177** (1995), no. 3, 847–869.

[4] D. MacHale, *Sequence A001292 in the On-line Encyclopedia of Integer Sequences (n.d.)*, `https://oeis.org/A046668`, Accessed on Jan 17 2024.

[5] Desmond MacHale, *How commutative can a non-commutative group be?*, The Mathematical Gazette **58** (1974), no. 405, 199–202.

**Robert Heffernan** is a lecturer in Mathematics at MTU.
**Des MacHale** is an emeritus professor of Mathematics at UCC.

(R. Heffernan) Department of Mathematics, Bishopstown Campus, Munster Technological University

(D. MacHale) Department of Mathematics, University College Cork
*E-mail address*, R. Heffernan: `robert.heffernan@mtu.ie`
*E-mail address*, D. MacHale: `d.machale@ucc.ie`