Publ. Mat. (2007), 181–191
Proceedings of the *Primeras Jornadas de Teoría de Números*.

SOME PROBLEMS IN NUMBER THEORY THAT ARISE FROM GROUP THEORY

Alexander Moretó

Abstract

In this expository paper, we present several open problems in number theory that have arisen while doing research in group theory. These problems are on arithmetical functions or partitions. Solving some of these problems would allow to solve some open problem in group theory.

1. Introduction

Recently, while doing research in group theory, I have reduced some of the problems I was considering to problems in number theory for which I have been unable to find a solution. Similarly, there are also many examples of problems that other group theorists have reduced to questions in number theory. These are well-known and important problems for group theorists, but given that their origin lies far away from number theory, they do not seem to be as well-known as they deserve to be among number theorists. The goal of this expository paper, therefore, is to make some of these problems known in the number theory community. We hope that this will eventually allow to solve at least some of them.

The number theoretical problems that we will consider may be divided into two types. One of them are problems on partitions and Young diagrams. These problems arise naturally when studying the complex irreducible character degrees of symmetric groups.

2000 *Mathematics Subject Classification.* 11A25, 11A41, 11A51, 11N37, 11N56, 11P81, 11P82, 11P83, 20C15, 20C30, 20D60.
Key words. Partition, symmetric group, character degree, irreducible character, arithmetical function.
Research supported by the Spanish Ministerio de Educación y Ciencia, MTM2004-06067-C02-01 and MTM2004-04665, the FEDER and Programa Ramón y Cajal.

The other type of problems refers to the classical arithmetical functions of number theory. In the last decades there has been a strong interest in the study of the so called arithmetical structure of finite groups. Some of these questions reduce to problems on the classical arithmetical functions.

This type of problems will be described in Section 3. In Section 2 we present the problems related to partitions and Young diagrams. For more motivation and details on the origin of the problems we refer the reader to the beginning of each of these sections.

I thank G. Glauberman, G. Malle and K. Ono for helpful comments on an earlier version of this paper.

2. Partitions and Young diagrams

An (ordinary) *representation* of a finite group G is a group homomorphism $\mathfrak{X}\colon G \to \mathrm{GL}(n,\mathbb{C})$ for some positive integer n. The *character* associated to the representation $\mathfrak{X}$ is the map $\chi\colon G \to \mathbb{C}$ defined by $\chi(g) = \mathrm{trace}\ \mathfrak{X}(g)$. The character χ is *irreducible* if it cannot be written as the sum of two characters. The degree of the character χ is the value $\chi(1)$ which, of course, is the size of the matrices of the associated representation. One of the basic facts in character theory is that the number of irreducible characters of a group G coincides with the number of conjugacy classes of G. For background on character theory of finite groups, we refer the reader to [**17**]. With the hope of getting a better understanding of the ordinary characters, R. Brauer introduced the modular characters and the p-blocks (as usual, in this paper we write p to denote a prime number). For background on modular character theory, we refer the reader to [**28**]. To understand this paper, it will suffice to know that a group G has a p-block of defect zero if and only if it has an irreducible character such that $\chi(1)_p = |G|_p$. In this case, χ is the unique ordinary irreducible character of the block.

A very important class of finite groups are the symmetric groups. A basic fact in group theory is that two elements of the symmetric group S_n belong to the same conjugacy class if and only if when we write them as a product of disjoint cycles they have the same number of t-cycles for every t. Therefore the number of conjugacy classes of S_n, and hence the number of irreducible characters of S_n, is the number of partitions of n.

In the first decades of the 20th century A. Young described a very nice correspondence between partitions of n and irreducible characters of S_n. Since Young's work, the representation theory of symmetric groups has been an active area of research. As pointed out in [**20**], one reason for

this is that symmetric groups have served as a good source of inspiration for the study of representations of other classes of groups and algebras (see, for instance, Corollary 5.38 of [**22**], [**8**], or [**20**]). For a detailed account of the most important results until 1980 we refer the reader to [**19**].

For the purpose of this paper, we are interested in the degrees of the irreducible characters of S_n. Given a partition of n, $\mu = (a_1, \ldots, a_t)$, with $a_1 \geq a_2 \geq \cdots \geq a_t$, the Young diagram associated to μ is an array of n nodes with a_i nodes in the ith row. We assign numbers to the rows and columns and coordinates to the nodes. The *hook number* $H(i,j)$ of the node (i,j) is the number of nodes to the right and below the node (i,j), including the node (i,j). The degree of the character χ_μ associated to the partition μ is given by the *hook length formula*

$$\chi_\mu(1) = \frac{n!}{\prod_{i,j} H(i,j)}.$$

This description of the degrees was obtained by J. S. Frame, G. de B. Robinson and R. M. Thrall in [**12**].

With this formula, it becomes clear that any problem on degrees of irreducible characters of symmetric groups depends on results on partitions. For instance, it follows from the t-core partition conjecture that alternating groups have a p-block of defect zero for all primes $p \geq 5$. A *t-core partition* of n is a partition of n in which none of the hook numbers is divisible by t. The t-core partition conjecture asserts that for every $t \geq 4$, every integer n has a t-core partition. Using the theory of modular forms, the proof of this conjecture was completed in [**14**]. See the references in [**14**] for previous work on this conjecture. This, in turn, allowed A. Granville and K. Ono to complete the classification of finite simple groups with defect zero p-blocks. In fact, they proved a stronger result in the case of alternating (or symmetric) groups: for every prime $p \geq 5$ the number of defect zero p-blocks goes to infinity when n goes to infinity.

One of the most important problems in representation theory of finite groups is McKay's conjecture, which asserts that the number of irreducible characters of a group G whose degree is not divisible by p (the so called characters of p'-degree) coincides with the number of characters of p'-degree of the normalizer of a Sylow subgroup. This description of the character degrees of the symmetric groups allowed J. B. Olsson to solve McKay's conjecture for symmetric groups in [**29**]. Recently, a strengthening of McKay conjecture was formulated by I. M. Isaacs and

G. Navarro in [**18**]. This strong form of McKay's conjecture was proved for symmetric groups by P. Fong in [**11**].

The number of irreducible characters of a group G whose degree has a given p-part is also interesting and it is the origin of other conjectures in group representation theory. These numbers are known as *McKay numbers*. In the case of symmetric groups they have recently been studied by K. Ono in [**31**], where he proved that the Ramanujan congruences for the partition function modulo 5, 7, 11, 25, 49 and 121 (see [**5**]) descend to congruences of McKay numbers. By the work of S. Ahlgren and K. Ono [**1**], [**2**], [**30**] it is now known that there are Ramanujan type congruences for every modulus M coprime to 6. A natural question (see Question 1 of [**31**]) is which of these congruences descend to McKay numbers. It would be interesting to consider whether these results may have applications to the representation theory of symmetric groups.

Now, we will begin to describe some open problems in number theory that have arosen from problems in the representation theory of symmetric groups. In [**24**], we studied Brauer's Problem 1 [**6**]. This problem asks the following: What are the complex group algebras of finite groups? A classical theorem of Wedderburn asserts that the group algebra of a finite group G is

$$\mathbb{C}G = \bigoplus_{i=1}^{k} M(n_i, \mathbb{C})$$

where $M(n_i, \mathbb{C})$ is the algebra of complex matrices of size n_i, $n_i = \chi_i(1)$ and the set of irreducible characters of G is $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$. Thus, Brauer's Problem 1 asks for the possible sets of degrees with multiplicities of finite groups. It seems that with today's knowledge of representation theory, it is not possible to settle this question. But we think that it should be possible to obtain some partial results. The first of these partial results, which we discuss now, appears in [**24**]. We conjectured that the order of a finite group is bounded in terms of the largest multiplicity of the character degrees. The main result in [**24**] is that this conjecture is true for every finite group if it holds for symmetric groups. Therefore, this is an example of a problem where a result on partitions would allow to obtain properties of representations of *arbitrary* finite groups.

So our first problem is the following. Given a group G, we write $m(G)$ to denote the largest multiplicity of the character degrees of G.

Conjecture 2.1. *$m(S_n) \to \infty$ when $n \to \infty$.*

Given a partition of n, we can consider the lengths of the columns of the associated Young diagram. They form another partition of n, which

is called the associated partition. It is easy to see that most of the times the associated partition of a partition μ does not coincide with μ, so it yields a different irreducible character of S_n. But it is easy to see that the degrees of these two characters coincide. In this way, one can prove that $m(S_n) \geq 2$ for $n \geq 2$. For $n \geq 60$, M. Slattery has found some partitions that can be transformed in different partitions of n in such a way that the degree of the associated character is preserved. This has allowed him to show that $m(S_n) \geq 4$ for $n \geq 60$. Is it possible to find k degree preserving transformations of certain partitions on n for some k that goes to infinity when n goes to infinity?

It would also be interesting to know more precisely the asymptotic behavior of $m(S_n)$. Computer calculations suggest that, perhaps, $n/3 \leq m(S_n) < n$ for large n.

One reason why we believe that it might be difficult to prove Conjecture 2.1 is that $m(S_n)$ is not monotonic. Even the following weak version of Conjecture 2.1 would be interesting.

Conjecture 2.2. $\limsup m(S_n) = \infty$.

Given a group G, we write $\mathrm{cd}(G)$ to denote the set of degrees of the irreducible characters of G. By the classical result of Hardy and Ramanujan [**15**] on the number of partitions, we have that $|\mathrm{Irr}\,(S_n)|$, the number of irreducible characters of S_n, is asymptotically equivalent to

$$(1/4n\sqrt{3})\exp(\pi\sqrt{2n/3}).$$

One way to prove Conjecture 2.1 would be to prove that $|\mathrm{Irr}\,(S_n)|/|\mathrm{cd}\,(S_n)| \to \infty$ when $n \to \infty$, but computer calculations indicate that this is probably false. We have checked that for $5 \leq n < 55$,

$$1.75 \leq |\mathrm{Irr}\,(S_n)|/|\mathrm{cd}\,(S_n)| \leq 2.525$$

so it seems likely that the asymptotic behavior of $|\mathrm{cd}\,(S_n)|$ is similar to that of the number of partitions.

Question 2.3. *What is the asymptotic behavior of* $|\mathrm{cd}\,(S_n)|$*?*

We remark that this question has recently been considered, and solved, for the other infinite families of simple groups, i.e., for groups of Lie type [**21**]. In [**21**] it was also asked whether or not Conjecture 2.1 is true.

Our computer calculations also suggest that for large n if $d \in \mathrm{cd}(S_n)$ the probability that d occurs with multiplicity 2 is bigger than 0.8 and the probability that it occurs with multiplicity larger than 6 is less than 0.02. Given d, we write $m(d)$ to denote the multiplicity of d as a character degree of S_n.

Problem 2.4. *Find reasonable values of ε_1 and ε_2 such that*

$$P(m(d) = 2 \mid d \in \mathrm{cd}(S_n)) \geq 1 - \varepsilon_1$$

for n sufficiently large and

$$P(m(d) > 6 \mid d \in \mathrm{cd}(S_n)) \leq \varepsilon_2$$

for n sufficiently large.

We conclude this section by remarking that the first two problems that we will consider in the next section are also related to questions on character degrees of symmetric groups and, therefore, partitions and Young diagrams.

3. Arithmetical functions

Let $n = p_1^{a_1} \dots p_t^{a_t}$ be a positive integer written as a product of powers of pairwise different primes. Following [**16**], we define

$$\begin{aligned} &\omega(n) = t, \\ &\Omega(n) = a_1 + \cdots + a_t, \qquad \text{and} \\ &d(n) = (a_1 + 1) \dots (a_t + 1), \end{aligned}$$

i.e., ω, Ω and d count, respectively, the number of different prime divisors, the total number of prime factors and the total number of divisors of n.

The problems on the arithmetical structure of finite groups ask the following type of questions: In what way does the number of prime divisors of the irreducible character degrees of a group (or conjugacy class sizes, or element orders,...) restrict the structure of the group? We refer the reader to [**32**] for a survey on these problems from a group theoretical point of view.

A typical example of a problem on the arithmetical structure of finite groups is Huppert's $\rho - \sigma$ conjecture. Given a group G, $\rho(G)$ is the set of primes that divide the degree of some irreducible character and

$$\sigma(G) = \max\{\omega(\chi(1)) \mid \chi \in \mathrm{Irr}(G)\}.$$

Huppert's $\rho - \sigma$ conjecture says the following.

(i) If G is solvable, then $|\rho(G)| \leq 2\sigma(G)$.

(ii) There exists an integer valued function such that for arbitrary groups $|\rho(G)| \leq f(\sigma(G))$.

Huppert's $\rho - \sigma$ conjecture was proved for simple groups by Alvis and Barry in [**4**]. In that paper, they conjecture that the following strong form of their results hold.

Conjecture 3.1. *For $n \geq 15$, there exists an irreducible character of the symmetric group S_n whose degree is a multiple of all the prime divisors of $n!$*

This has been checked with computer for $15 \leq n \leq 100000$. See [**4**] for a more detailed discussion on this conjecture.

A question of a similar flavor, even though a different origin, is the following.

Question 3.2. *Does there exist a constant c such that for every integer n there exist $\chi_1, \ldots, \chi_c \in \mathrm{Irr}(S_n)$ with $\chi_1(1) \ldots \chi_c(1)/n!$ an integer?*

This has been proved in [**25**] for the remaining families of finite simple groups with $c = 5$. A similar result was proved in [**27**] for solvable groups.

An affirmative answer to Question 3.2 would allow to improve considerably the bound in the main result of [**25**], which refers to arbitrary finite groups. A well-known theorem of Gluck [**13**] asserts that every finite group has an abelian subgroup A such that $|G : A|$ is bounded in terms of the largest degree of the irreducible characters of G. The main result in [**25**] provides a bound for $\Omega(|G : A|)$ for some abelian A in terms of $\max_{\chi \in \mathrm{Irr}(G)} \Omega(\chi(1))$.

Many results and conjectures on character degrees have analogs on conjugacy class sizes. For instance, there is also the $\rho - \sigma$ problem for conjugacy classes. Let $\rho^*(G)$ be the set of primes that divide the size of some conjugacy class of G and

$$\sigma^*(G) = \max\{\omega(|C|) \mid C \in \mathrm{Cl}(G)\},$$

where $\mathrm{Cl}(G)$ is the set of conjugacy classes of G. It is known that there cannot be any bound better than $|\rho^*(G)| \leq 3\sigma^*(G)$ for solvable groups. The best known bound is $|\rho^*(G)| \leq 4\sigma^*(G)$ (see [**33**]). (The coefficient 4 can be lowered to 3.5 for odd order groups by [**27**].) As remarked by Zhang, the bound $|\rho^*(G)| \leq 3\sigma^*(G)$ would follow from an affirmative answer to the following question.

Question 3.3. *Let $m_1, \ldots, m_n > 1$ be pairwise coprime positive integers and $q_1, \ldots, q_n$ be n arbitrary prime powers. Is it true that*

$$\omega\left(\prod_{i=1}^{n} \frac{q_i^{m_i} - 1}{q_i - 1}\right) \geq n?$$

Of course, it is no loss of generality to assume that the m_i's are prime numbers.

In a celebrated paper, W. Feit and J. G. Thompson [**10**] proved that odd order groups are solvable. An affirmative answer to the following conjecture of Thompson (see Problem 4.65 of [**23**]), would allow to simplify part of the proof.

Conjecture 3.4. *Let $p \neq q$ be two prime numbers. Then $\frac{p^q-1}{p-1}$ never divides $\frac{q^p-1}{q-1}$.*

One of the infinite families of finite simple groups are the projective special linear groups. Their order is given by the formula

$$|\mathrm{PSL}\,(n,q)| = \frac{q^{n(n-1)/2}}{(n,q-1)}(q^2-1)(q^3-1)\ldots(q^n-1).$$

Here q is a power of a prime p. See [**7**] for the order formulas of the other families of simple groups of Lie type. For the alternating groups on $n \geq 3$ letters it is well-known that $|A_n| = n!/2$. The asymptotic behavior of the number of divisors of $n!$ was found out in [**9**]. This result was useful in [**24**]. It would be convenient to have related results for the number of divisors of the ordesr of the remaining families of simple groups.

In the following problems, "asymptotic behavior" has three possible meanings, all of them interesting: as $n \to \infty$ and q is a prime power that goes to ∞ or as $|G| \to \infty$.

Problem 3.5. *Study the asymptotic behavior of $d(|G|)$ when G is a projective special linear group. The same for the other families of simple groups of Lie type.*

Similarly, it would also be convenient to know the following.

Problem 3.6. *Study the asymptotic behavior of $\omega(|G|)$ and $\Omega(|G|)$ when G is a projective special linear group. The same for the other families of simple groups of Lie type. In particular, what is the relation between $\omega(|\mathrm{PSL}\,(n,q)|_{p'})$ and $\max_{i=1}^{n}\omega(q^i-1)$?*

It is possible that results of this type would allow to improve the bounds in [**26**], where the number of prime divisors of the order of a finite group G is bounded in terms of the maximum number of prime divisors of the order of an element. For a somehow related theorem and an application to group theory, see [**3**].

Notes added in proof: i) Conjecture 2.1 (and hence Conjecture 2.2) has now been proved in: D. Craven, Symmetric group character degreees and hook numbers, preprint.

ii) Conjecture 3.1 has been proved in: M. S. Barry and M. B. Ward, On a conjecture of Alvis, *J. Algebra* **294** (2005), 136–155.

References

[1] S. AHLGREN, Distribution of the partition function modulo composite integers M, *Math. Ann.* **318(4)** (2000), 795–803.

[2] S. AHLGREN AND K. ONO, Congruence properties for the partition function, *Proc. Natl. Acad. Sci. USA* **98(23)** (2001), 12882–12884 (electronic).

[3] K. ALLADI, R. SOLOMON AND A. TURULL, Finite simple groups of bounded subgroup chain length, *J. Algebra* **231(1)** (2000), 374–386.

[4] D. L. ALVIS AND M. J. J. BARRY, Character degrees of simple groups, *J. Algebra* **140(1)** (1991), 116–123.

[5] G. E. ANDREWS, *"The theory of partitions"*, Reprint of the 1976 original, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1998.

[6] R. BRAUER, Representations of finite groups, in: *"Lectures on Modern Mathematics"*, Vol. I, Wiley, New York, 1963, pp. 133–175.

[7] J. H. CONWAY, R. T. CURTIS, S. P. NORTON, R. A. PARKER AND R. A. WILSON, *"Atlas of finite groups"*, Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray, Oxford University Press, Eynsham, 1985.

[8] H. ELLERS, Searching for more general weight conjectures, using the symmetric group as an example, *J. Algebra* **225(2)** (2000), 602–629.

[9] P. ERDÖS, S. W. GRAHAM, A. IVIĆ AND C. POMERANCE, On the number of divisors of $n!$, in: *"Analytic number theory"*, Vol. 1 (Allerton Park, IL, 1995), Progr. Math. **138**, Birkhäuser Boston, Boston, MA, 1996, pp. 337–355.

[10] W. FEIT AND J. G. THOMPSON, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.

[11] P. FONG, The Isaacs-Navarro conjecture for symmetric groups, Special issue celebrating the 80th birthday of Robert Steinberg, *J. Algebra* **260(1)** (2003), 154–161.

[12] J. S. FRAME, G. DE B. ROBINSON AND R. M. THRALL, The hook graphs of the symmetric groups, *Canadian J. Math.* **6** (1954), 316–324.

[13] D. GLUCK, The largest irreducible character degree of a finite group, *Canad. J. Math.* **37(3)** (1985), 442–451.

[14] A. GRANVILLE AND K. ONO, Defect zero p-blocks for finite simple groups, *Trans. Amer. Math. Soc.* **348(1)** (1996), 331–347.

[15] G. H. HARDY AND S. RAMANUJAN, Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc.* **17** (1918), 75–115.

[16] 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.

[17] I. M. ISAACS, *"Character theory of finite groups"*, Corrected reprint of the 1976 original [Academic Press, New York], Dover Publications, Inc., New York, 1994.

[18] I. M. ISAACS AND G. NAVARRO, New refinements of the McKay conjecture for arbitrary finite groups, *Ann. of Math. (2)* **156(1)** (2002), 333–344.

[19] G. JAMES AND A. KERBER, *"The representation theory of the symmetric group"*, With a foreword by P. M. Cohn, With an introduction by Gilbert de B. Robinson, Encyclopedia of Mathematics and its Applications **16**, Addison-Wesley Publishing Co., Reading, Mass., 1981.

[20] B. KÜLSHAMMER, J. B. OLSSON AND G. R. ROBINSON, Generalized blocks for symmetric groups, *Invent. Math.* **151(3)** (2003), 513–552.

[21] M. W. LIEBECK AND A. SHALEV, Character degrees and random walks in finite groups of Lie type, *Proc. London Math. Soc. (3)* **90(1)** (2005), 61–86.

[22] A. MATHAS, *"Iwahori-Hecke algebras and Schur algebras of the symmetric group"*, University Lecture Series **15**, American Mathematical Society, Providence, RI, 1999.

[23] V. D. MAZUROV AND E. I. KHUKHRO, EDS. *"Kourovskaya tetrad"*, [The Kourovka notebook], Nereshennye voprosy teorii grupp, [Unsolved problems in group theory], Fifteenth augmented edition, E. Rossiĭskaya Akademiya Nauk Sibirskoe Otdelenie, Institut Matematiki im. S. L. Soboleva, Novosibirsk, 2002.

[24] A. MORETÓ, On the structure of the complex group algebras of finite groups, submitted.

[25] A. MORETÓ, A variation on theorems of Jordan and Gluck, *J. Algebra* **301(1)** (2006), 274–279.

[26] A. MORETÓ, On the number of different prime divisors of element orders, *Proc. Amer. Math. Soc.* **134(3)** (2006), 617–619 (electronic).
[27] A. MORETÓ AND T. R. WOLF, Orbit sizes, character degrees and Sylow subgroups, *Adv. Math.* **184(1)** (2004), 18–36.
[28] G. NAVARRO, *"Characters and blocks of finite groups"*, London Mathematical Society Lecture Note Series **250**, Cambridge University Press, Cambridge, 1998.
[29] J. B. OLSSON, McKay numbers and heights of characters, *Math. Scand.* **38(1)** (1976), 25–42.
[30] K. ONO, Distribution of the partition function modulo m, *Ann. of Math. (2)* **151(1)** (2000), 293–307.
[31] K. ONO, Partitions and McKay numbers for S_n, *J. Combin. Theory Ser. A* **108(2)** (2004), 185–197.
[32] J. P. ZHANG, Some new results on arithmetical problems in the theory of finite groups, in: *"Groups '93 Galway/St. Andrews"*, Vol. 2, London Math. Soc. Lecture Note Ser. **212**, Cambridge Univ. Press, Cambridge, 1995, pp. 586–593.
[33] J. P. ZHANG, On the lengths of conjugacy classes, *Comm. Algebra* **26(8)** (1998), 2395–2400.

Departament d'Àlgebra
Universitat de València
46100 Burjassot, València
Spain
E-mail address: Alexander.Moreto@uv.es