hexagon:2611.01255v1

ON CONJUGACY CLASSES AND DIVISORS OF $p-1$

THOMAS MICHAEL KELLER

Abstract. It was observed by Çınarcı and Keller that the existence of finite groups with few conjugacy classes might be related to the existence of divisors of a certain size of $p-1$, where p is a prime divisor of the group order. We show that if p divides the index of the Fitting subgroup of a finite group G and $k(G)$ is of the order of $p/\log_2 p$, then $p-1$ necessarily has a divisor of the order of $\log_2 p$. We relate this result to the recent proof of the conjecture of Çınarcı and Keller by Çınarcı, Keller, Maróti and Simion, which in particular yields the sharp lower bound $(p+5)/2$ for safe primes in this situation. We also discuss the arithmetic of the examples arising from Mersenne primes.

1. Introduction

In this note we resolve a somewhat mysterious curiosity first observed in [2]. For a finite group G we denote by $k(G)$ the number of conjugacy classes of G and by $\mathrm{F}(G)$ the Fitting subgroup of G. All groups in this note will be finite, and throughout log means $\log_2$.

In [7, Theorem A], Moretó and the author proved that there is a universal constant $D>0$ such that if p is a prime dividing $|G:\mathrm{F}(G)|$, then

$$k(G) \geq D\frac{p}{\log p}.$$

If there are infinitely many Mersenne primes, then this bound is of the best possible order of magnitude. Indeed, if $p=2^q-1$ is a Mersenne prime and $G=\mathrm{A}\Gamma(2^q)$ is the corresponding affine semilinear group, then p divides $|G:\mathrm{F}(G)|$ and, as observed in [7, Section 1],

$$k(G) = \frac{p-1}{q}+2q = \frac{p-1}{\log(p+1)}+2\log(p+1). \tag{1}$$

In [2], Çınarcı and the author considered a different lower bound. For a prime p, let

$$m(p) = \min\left\{a+b \mid a,b\in\mathbb{N},\ ab=p-1\right\}.$$

Conjecture A of [2] asserted that if p divides $|G|$, then $k(G)\geq m(p)$, with equality if and only if $G\cong C_p\rtimes C_a$ or $G\cong C_p\rtimes C_b$, where $p-1=ab$, $a+b=m(p)$, and the complement acts faithfully on C_p. The conjecture was proved there for solvable groups and, using the McKay conjecture, for arbitrary groups and sufficiently large primes p. It has since been proved in full by Çınarcı, the author, Maróti and Simion in [3, Theorem 1.2], where in fact a stronger result is obtained. Namely, if $k_p(G)$ denotes the number of conjugacy classes of nonidentity p-elements and $k_{p'}(G)$ the

2020 *Mathematics Subject Classification.* Primary 20E45; Secondary 20D25, 20C15, 11A41.

Key words and phrases. Finite groups, conjugacy classes, Fitting subgroup, Mersenne primes, safe primes.

number of conjugacy classes of p'-elements (including the identity), then, with one exception, there is a factorization $p-1=cd$ such that

$$k_p(G) \geq c \qquad \text{and} \qquad k_{p'}(G) \geq d,$$

with equality in both inequalities if and only if $G \cong C_p \rtimes C_d$ with $C_G(C_p) = C_p$. The exception is $p = 11$ and $G \cong (C_{11} \times C_{11}) \rtimes \mathrm{SL}(2,5)$ as in [3], in which case $k_{11}(G) = 1$ and $k_{11'}(G) = 9$. Since $m(11) = 7$, this exception does not affect the assertion of Conjecture A, including its characterization of equality.

If $p \geq 5$ is a safe prime (i.e., $(p-1)/2$ is prime), then $m(p) = (p+3)/2$. Thus the examples in (1) raise a natural question about the arithmetic of the primes for which the bound in [7] is close to being attained. This was pointed out in Remark (8) following Conjecture A in [2].

Even now that Conjecture A has been proved, the question raised in that remark is not entirely settled. While the bound $k(G) \geq m(p)$ implies the existence of a sufficiently large divisor of $p-1$ when $k(G)$ is small, it does not by itself give a logarithmic upper bound for the size of such a divisor. The purpose of this note is to show that, under the hypothesis of [7], the phenomenon suggested in that remark does indeed occur. More precisely, we prove the following.

Theorem A. *For every real number $C > 0$ there exist positive constants c_1, c_2 and p_0 such that the following holds. If $p > p_0$ is a prime, G is a group such that p divides $|G : \mathrm{F}(G)|$, and*

$$k(G) \leq C\frac{p}{\log p},$$

then $p-1$ has a divisor d such that

$$c_1 \log p \leq d \leq c_2 \log p.$$

Moreover, c_2 can be chosen independently of C.

For safe primes the recent result in [3] gives an especially nice improvement of the bound in [7, Theorem A]. We record it here as a direct consequence of that result.

Theorem B. *If p is a safe prime and G is a group such that p divides $|G : \mathrm{F}(G)|$, then*

$$k(G) \geq \frac{p+5}{2}.$$

This bound is sharp for every safe prime p.

We first prove Theorem A, then establish Theorem B using [3], and finally return to the examples in (1). We emphasize that the hypotheses of Theorems A and B concern prime divisors of $|G : \mathrm{F}(G)|$, rather than merely prime divisors of $|G|$.

2. Proofs of Theorems A and B

The following lemma makes explicit an observation implicit in the proofs of Theorems 4.2 and 4.3 of [7].

Lemma 2.1. *There exist universal constants $\epsilon \in (0,1)$, $\beta > 0$ and $\delta > 0$ such that if p is a prime dividing $|G : \mathrm{F}(G)|$ and $k(G) < \epsilon p$, then there is a positive divisor d of $p-1$ such that*

$$k(G) \geq d + \frac{p-1}{d} \quad \text{and} \quad k(G) \geq 2^{\beta d - 16\delta(\log d)^4}. \tag{2}$$

Proof. By [7, Theorems B and 2.2 and Lemma 4.1], we can choose $\epsilon \in (0,1)$ sufficiently small so that groups under consideration are p-solvable, have Sylow p-subgroups of order p, and cannot be groups as in that Lemma 4.1. The same exclusions apply to quotients with p dividing the index of their Fitting subgroup.

Replacing G by a quotient of smallest order for which p still divides the index of the Fitting subgroup, we may assume that every proper quotient of G either has order coprime to p or has a normal Sylow p-subgroup. Here we use that the image of a Sylow p-subgroup still has order at most p, and that such a subgroup is contained in the Fitting subgroup if and only if it is normal. Also, $k(G)$ does not increase under this replacement.

We claim that G has a unique minimal normal subgroup V. Indeed, if V_1, V_2 were distinct minimal normal subgroups, then G would embed into $G/V_1 \times G/V_2$. The latter group has a normal Sylow p-subgroup, and hence so does each of its subgroups, a contradiction. Moreover, p does not divide $|V|$: otherwise, by p-solvability, V would be an elementary abelian group of order p, again a contradiction. By our choice of ϵ and [7, Lemma 4.1], V must be abelian.

By the usual Fitting subgroup formula for the Frattini quotient (see [5, III, 4.2(d)]), we have $\Phi(G) = 1$. Thus there is a maximal subgroup H not containing V, and $G = HV$. As V is abelian, $H \cap V$ is normal in G, so $H \cap V = 1$. Also $C_H(V)$ is normal in G and intersects V trivially, whence $C_H(V) = 1$ by uniqueness of V. Thus V is a faithful irreducible H-module over a field of prime order $r \neq p$. By the choice of G, the Sylow p-subgroup P of $H \cong G/V$ is normal in H and has order p.

Now put $M = C_H(P)$ and $d = |H : M|$. Clearly H/M is cyclic and d divides $p-1$. Also $M = P \times K$ for a Hall p'-subgroup K of M, since P is central in M. Counting the classes in the nonidentity elements of P, and the classes mapping onto the nonidentity elements of H/M (or simply the classes in the Frobenius quotient H/K), yields

$$k(G) \geq k(H) \geq d + \frac{p-1}{d}.$$

Here K is characteristic in M and hence normal in H.

For completeness we give the argument for the second inequality, following [7, proof of Theorem 4.2]. First observe that $|V| \geq 2^d$. Indeed, over an algebraic closure of the field of order r, the nontrivial eigencharacters of P occurring on V are permuted by H. At least one occurs by faithfulness. Each such eigencharacter has an orbit of length d, since the stabilizer in H of any nontrivial character of the cyclic group P of prime order is M. Thus $\dim_{\mathbb{F}_r} V \geq d$, as desired.

Let S be the solvable radical of H. The solvable group SV has trivial Frattini subgroup: by Clifford's theorem V is completely reducible as an S-module, so the maximal subgroups obtained by adjoining S to maximal proper S-submodules of V have intersection S. Consequently $\Phi(SV) \cap V = 1$ and $\Phi(SV)$ centralizes V. Since $C_{SV}(V) = V$, we obtain $\Phi(SV) = 1$. By [6, Theorem B], for some universal constant $\beta > 0$ we now have

$$k(SV) \geq |SV|^\beta \geq 2^{\beta d}. \tag{3}$$

Next, by the usual inequality $k(M) \leq |H : M| k(H)$ (see [4]),

$$pk(K) = k(M) \leq dk(H) < dp,$$

so $k(K) \leq d$. Since $P \leq S$, we get $MS/S \cong K/(K \cap S)$ and hence $k(MS/S) \leq d$. Using $k(H/MS) \leq d$ and the standard bound on the class number in terms of a normal subgroup and its quotient, we obtain $k(H/S) \leq d^2$.

As H/S has trivial solvable radical, [1, Theorem 2.1], in the form used in [7, proof of Theorem 4.2], gives a universal constant $\delta > 0$ such that

$$\log |H/S| \leq \delta(\log k(H/S))^4 \leq 16\delta(\log d)^4.$$

The inequality also holds if $H = S$. Putting this together with (3), we obtain

$$k(G) \geq \frac{k(SV)}{|H:S|} \geq 2^{\beta d - 16\delta(\log d)^4},$$

as wanted. Since passing to the quotient at the beginning can only decrease the class number, both inequalities hold for the original group. □

Proof of Theorem A. Let ϵ, β, δ be as in Lemma 2.1. For sufficiently large p we have $C/\log p < \epsilon$, so the lemma applies. Its first inequality yields

$$d \geq \frac{p-1}{k(G)} \geq \frac{p-1}{Cp} \log p \geq \frac{1}{2C} \log p. \tag{4}$$

In particular, we may assume that d is sufficiently large so that $16\delta(\log d)^4 \leq \beta d/2$. Thus by the second inequality in (2) we find that

$$p > k(G) \geq 2^{\beta d/2},$$

whence $d \leq (2/\beta) \log p$. The theorem follows with $c_1 = 1/(2C)$ and $c_2 = 2/\beta$. □

Proof of Theorem B. By the bound and the characterization of equality established in [3, Theorem 1.2], if p divides $|G : \mathrm{F}(G)|$, then

$$k(G) > m(p).$$

Indeed, the groups attaining $m(p)$ all have a normal Sylow p-subgroup, which is therefore contained in their Fitting subgroup. In the exceptional case of [3, Theorem 1.2], we also have strict inequality, as noted in Section 1. Since p is a safe prime, $m(p) = (p+3)/2$, and the desired bound follows by integrality.

For sharpness, take $G = \mathrm{PSL}(2, p)$. As $p \geq 5$, this is a nonabelian simple group of order divisible by p, so $\mathrm{F}(G) = 1$. Moreover, $k(G) = (p+5)/2$ (see Remark (7) following Conjecture A in [2]). Thus equality is attained for every safe prime. □

3. The Mersenne prime examples

We now make a few observations on the arithmetic underlying (1). In fact the sharp bound $m(p)$, now established for all finite groups by [3], is of a quite different order of magnitude for Mersenne primes.

Theorem C. *Let $p = 2^q - 1$ be a Mersenne prime and let $G = \mathrm{A}\Gamma(2^q)$. Then the following hold.*

(a) *q divides $p - 1$ and $k(G) \geq m(p) + q$. If $q \geq 5$, then $6q$ divides $p - 1$.*
(b) *The only Mersenne prime which is a safe prime is 7.*
(c) *If $q \geq 3$, then*

$$2\sqrt{p-1} \leq m(p) \leq 3\sqrt{(p+1)/2} + 1.$$

In particular, if there are infinitely many Mersenne primes, then along these primes $m(p)$ is of the order of $\sqrt{p}$ and $k(G)/m(p) \to \infty$.

Proof. Clearly q is prime, and by Fermat's little theorem we have $q \mid 2^{q-1}-1$, whence $q \mid p-1$. Thus $m(p) \le q + (p-1)/q$ and (1) yields $k(G) \ge m(p)+q$. If $q \ge 5$, then q is odd, so $3 \mid 2^{q-1}-1$, and as $p-1 = 2(2^{q-1}-1)$ we see that $6q \mid p-1$. This proves (a).

For (b) and (c) suppose first that q is odd and put $u = 2^{(q-1)/2}$. Then

$$p - 1 = 2(u-1)(u+1). \tag{5}$$

If $q \ge 5$, both $u-1$ and $u+1$ are greater than 1, so $(p-1)/2$ is not prime. For $q=2$ and $q=3$ we obtain $p=3$ and $p=7$, respectively, of which only the latter is safe. This proves (b).

Now (5) gives the factorization $p-1 = (u-1)\cdot 2(u+1)$ and hence $m(p) \le 3u+1$. As $u = \sqrt{(p+1)/2}$, this is the desired upper bound in (c), whereas the lower bound is immediate from the arithmetic-geometric mean inequality. Finally (1) gives $k(G) \ge (p-1)/\log(p+1)$, and the last assertion follows. □

We close with two remarks.

(1) The inequality $k(G) \ge m(p)$ established in [3] by itself does not explain the existence of a divisor of $p-1$ of the order of $\log p$. Indeed, suppose that p divides $|G|$ and $k(G) \le Cp/\log p$. Writing $m(p) = a+b$ with $a \le b$, we get $a \ge (p-1)\log p/(Cp)$ and $a \le \sqrt{p-1}$. This only gives a lower bound of logarithmic size for a, not a logarithmic upper bound for any divisor. Even the stronger inequalities of [3, Theorem 1.2] give, directly, only the bounds $(p-1)/k(G) \le c, d \le k(G)$ for the two factors c, d (outside the exceptional case). In Theorem A the latter bound comes from the action on a minimal normal subgroup of a suitable quotient of G.

(2) In view of Theorem A it would be interesting to know for which primes p having a divisor of $p-1$ of the order of $\log p$ one can actually construct a group G such that p divides $|G : \mathrm{F}(G)|$ and $k(G)$ is of the order of $p/\log p$. Theorem A only establishes a necessary condition.

AI statement. This manuscript was drafted with the assistance of OpenAI's ChatGPT. The author devised the research question and had some ideas towards the solution and originally intended to use this as a student research project. But given the advent of powerful AI systems this seemed to be no longer a good project for students, and so the author used AI to perform the formal derivation and exposition of the results in this note. All arguments were subsequently checked by the author, who takes full responsibility for the content of this paper.

Funding declaration

Thie research was supported by a grant from the Simons Foundation (SFI-MPS-TSM-00014153 to Thomas M. Keller).

Disclosure statement

The author reports no conflict of interest.

Data availability

No data were used in this work.

References

[1] B. Baumeister, A. Maróti and H. P. Tong-Viet, Finite groups have more conjugacy classes, *Forum Math.* **29** (2017), 259–275.
[2] B. Çınarcı and T. M. Keller, A new lower bound for the number of conjugacy classes, *Proc. Amer. Math. Soc.* **152** (2024), 3757–3764.
[3] B. Çınarcı, T. M. Keller, A. Maróti and I. I. Simion, More on Landau's theorem and conjugacy classes, *Quart. J. Math.* **77** (2026), 679–705, doi: 10.1093/qmath/haag024.
[4] P. X. Gallagher, The number of conjugacy classes of a finite group, *Math. Z.* **118** (1970), 175–179.
[5] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin–Heidelberg–New York, 1967.
[6] T. M. Keller, Finite groups have even more conjugacy classes, *Israel J. Math.* **181** (2011), 433–444.
[7] T. M. Keller and A. Moretó, Prime divisors and the number of conjugacy classes of finite groups, *Math. Proc. Cambridge Philos. Soc.* **176** (2024), 1–16.

Department of Mathematics, Texas State University, 601 University Drive, San Marcos, Texas 78666, USA
Email address: keller@txstate.edu