http://ijgt.ui.ac.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 15 No. 3 (2026), pp. 123–134.

www.ui.ac.ir

COUNTING CONJUGACY CLASSES OF SUBGROUPS OF $\mathrm{PSL}_2(p)$

GARETH A. JONES

Abstract. This work is motivated by results obtained and problems posed by Bianchi, Camina, Lewis, Pacifici and Sanus, counting conjugacy classes of non-self-normalising subgroups of finite groups. We obtain formulae for the numbers of isomorphism and conjugacy classes of non-identity proper subgroups of the groups $G = \mathrm{PSL}_2(p)$, p prime, and for the numbers of those conjugacy classes which do or do not consist of self-normalising subgroups. The formulae are used to prove lower bounds 17, 18, 6 and 12 respectively satisfied by these invariants for all $p > 37$. A computer search carried out for a different but related problem shows that these bounds are attained for over a million primes p; we show that if the Bateman–Horn Conjecture is true, they are attained for infinitely many primes. Also, assuming no unproved conjectures, we use a result of Heath-Brown to obtain upper bounds for these invariants, valid for an infinite set of primes p.

1. Introduction

The aim of this note is to consider the following invariants of a finite group G:

(i) $i(G)$, the number of isomorphism classes of non-identity proper subgroups H of G;
(ii) $c(G)$, the number of conjugacy classes of such subgroups H of G;
(iii) $s(G)$, the number of conjugacy classes of such self-normalising subgroups H of G;
(iv) $n(G)$, the number of conjugacy classes of such non-self-normalising subgroups H of G.

MSC(2010): Primary: 20D99; Secondary: 11N32, 20D60, 20E32, 20G40.

Keywords: Projective special linear group, conjugacy classes of subgroups, self-normalising subgroups, Bateman–Horn Conjecture.

Article Type: Research Paper.

Communicated by Gunnar Traustason.

Received: 26 January 2025, Accepted: 30 July 2025, Published Online: 30 September 2025.

Cite this article: G. A. Jones, Counting conjugacy classes of subgroups of $\mathrm{PSL}_2(p)$, *Int. J. Group Theory*, **15** no. 3 (2026) 123–134. https://dx.doi.org/10.22108/ijgt.2025.144154.1942 .

A subgroup $H \leq G$ is *self-normalising* if H coincides with its normaliser $N_G(H)$. The motivation for this paper was a seminar by Mark Lewis [14] on $n(G)$ (a preprint [3] gives full details, with $n(G)$ denoted there by $\mathcal{D}(G)$). The main theme was that a low value of this invariant imposes strong restrictions on G; for example, if $n(G) \leq 3$ then G is solvable, of derived length at most 2, while A_5 is the only nonsolvable group with $n(G) = 4$. The seminar was mainly about solvable groups, but it raised further questions about the values of $n(G)$ for non-abelian finite simple groups, answered partially here in Theorems 1.3 and 1.4.

Using Dickson's description [8, Ch. XII] of the subgroups of $\mathrm{PSL}_2(q)$, where q is a prime power (see also [10, §II.8]) we will give formulae in equations (2.1) to (2.4) of Section 2 for these invariants for the groups $G = \mathrm{PSL}_2(p)$ (p prime). As a consequence, we will prove the following:

Theorem 1.1. *The groups $G = \mathrm{PSL}_2(p)$, p prime, satisfy*

(i) $i(G) \geq 17$ *for all* $p \geq 29$*;*
(ii) $c(G) \geq 18$ *for all* $p \geq 23$*;*
(iii) $s(G) \geq 6$ *for all* $p \geq 41$*;*
(iv) $n(G) \geq 12$ *for all* $p \geq 23$.

The exceptions for small p can be seen in Table 1, at the end of Section 2, which lists the values of these invariants for primes $p = 3, \ldots, 61$. It is of interest to know whether the lower bounds in Theorem 1.1 are sharp. A computer search reported in [12], in relation to a different problem concerning the groups $\mathrm{PSL}_2(p)$, found a set of more than 1.2×10^6 primes p for which all four lower bounds are attained. In fact, we make the following conjecture:

Conjecture 1.2. *There is an infinite set of primes p for which the groups $G = \mathrm{PSL}_2(p)$ satisfy $i(G) = 17$, $c(G) = 18$, $s(G) = 6$ and $n(G) = 12$.*

A proof of this conjecture would depend on a certain triple of polynomials in $\mathbb{Z}[t]$ simultaneously taking prime values for infinitely many $t \in \mathbb{N}$. This sort of problem is the subject of the Bateman–Horn Conjecture (BHC), which gives estimates for the number of $t \leq x$, for large x, giving prime values to a given finite set of polynomials. In all known applications these estimates agree closely with data from computer searches: for example, see [11, 12] for other applications to group theory. This gives strong evidence (but at present no proof) that the BHC is true, and hence that Conjecture 1.2 is correct. Thus our second main result is the following:

Theorem 1.3. *If the BHC is true then there is an infinite set of primes p for which the lower bounds 17, 18, 6 and 12 in Theorem 1.1 are attained.*

In the absence of the BHC and any other unproved conjectures, we are able to use a result of Heath-Brown [6] to prove the following much weaker result:

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

Theorem 1.4. *There is an infinite set of primes p for which the groups $G = \mathrm{PSL}_2(p)$ satisfy*

(i) $i(G) \leq 390$*;*
(ii) $c(G) \leq 454$*;*
(iii) $s(G) \leq 132$*;*
(iv) $n(G) \leq 384$.

The existence of an infinite set of non-abelian finite simple groups G with $n(G)$ bounded above answers a question raised by Lewis in [14]. The large gaps between the bounds in Theorems 1.1 and 1.4 suggest that there is further work to be done in reducing these upper bounds.

2. Subgroups of $\mathrm{PSL}_2(p)$

By Dickson's description [8, Ch. XII] of the subgroups of $\mathrm{PSL}_2(q)$, we have the following:

Lemma 2.1. *For any prime $p > 2$ the isomorphism types of non-identity proper subgroups of $G := \mathrm{PSL}_2(p)$ are as follows, where δ and ε are the numbers of divisors d and e of $(p \pm 1)/2$ respectively: .*

(1) C_d *and* D_d *for the divisors $d \neq 1$ of $(p+1)/2$, giving $\delta - 1$ types in either case;*
(2) C_e *and* D_e *for the divisors $e \neq 1$ of $(p-1)/2$, giving $\varepsilon - 1$ types in either case;*
(3) $\mathrm{C}_p \rtimes \mathrm{C}_e$ *for the divisors e of $(p-1)/2$, giving ε types;*
(4) A_4 *if $p \geq 5$;*
(5) S_4 *if $p \equiv \pm 1 \bmod (8)$;*
(6) A_5 *if $p \equiv \pm 1 \bmod (5)$.*

We will assume that $p \geq 5$. Adding up the above numbers, we see that the total number $i(G)$ of such isomorphism types is given by

$$i(G) = 2\delta + 3\varepsilon - 3 + \sigma + \alpha, \tag{2.1}$$

where $\sigma = 1$ or 0 as $p \equiv \pm 1$ or $\pm 3 \bmod (8)$, and $\alpha = 1$ or 0 as $p \equiv \pm 1 \bmod (5)$ or not.

An integer $n = p_1^{e_1} \cdots p_k^{e_k}$ (p_i distinct primes) has $\tau(n) = (e_1 + 1) \cdots (e_k + 1)$ divisors. Since the average value of $\tau(n)$ is approximately $\log n$ (see, for instance, [13, Theorem 6.30]), if we choose the prime p randomly, we should expect $(p \pm 1)/2$ each to have on average about $\log(p/2)$ divisors. It follows from de la Vallée-Poussin's quantified form of Dirichlet's Theorem (see [4, Ch. 5, §3.2], for instance) that σ and α each have average value $1/2$, so on average we have

$$i(G) \approx 5 \log p - 2.$$

However, we aim to choose primes p for which $(p \pm 1)/2$ each have a small number of divisors, so that $i(G)$ and the related invariants $c(G)$, $s(G)$ and $n(G)$ are as small as possible; more specifically, we want an infinite set of primes for which these invariants are uniformly bounded above. To see how small we can make these upper bounds, we will in the next section first look for lower bounds on

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

these invariants. In order to do this, we will now find formulae analogous to (2.1) for the remaining invariants.

By inspection of [8, Ch. XII], we have the following:

Lemma 2.2. *Each of the isomorphism types in Lemma 2.1 is represented by a single conjugacy class in G, with the following exceptions, each represented by two classes:*

(1) D_d *for those* $d \neq 1$ *dividing* $(p+1)/2$ *such that* $(p+1)/2d$ *is even;*
(2) D_e *for those* $e \neq 1$ *dividing* $(p-1)/2$ *such that* $(p-1)/2e$ *is even;*
(4) A_4 *if* $p \equiv \pm 1 \bmod (8)$*;*
(5) S_4 *if* $p \equiv \pm 1 \bmod (8)$*;*
(6) A_5 *if* $p \equiv \pm 1 \bmod (5)$.

The proportion of the divisors d or e of $(p \pm 1)/2$ with an even quotient is $k/(k+1)$ or $l/(l+1)$ where 2^k and 2^l are the highest powers of 2 dividing $(p \pm 1)/2$. Since $(p \pm 1)/2$ have opposite parity, either $k = 0$ or $l = 0$, as $p \equiv \pm 1 \bmod (4)$. In just one of these two cases the divisor 1 with even quotient must be excluded, so the number $c(G)$ of conjugacy classes of non-identity proper subgroups of G is given by

$$\begin{aligned} c(G) &= i(G) + \frac{k}{k+1}\delta + \frac{l}{l+1}\varepsilon - 1 + 2\sigma + \alpha \\ &= \left(2 + \frac{k}{k+1}\right)\delta + \left(3 + \frac{l}{l+1}\right)\varepsilon - 4 + 3\sigma + 2\alpha. \end{aligned} \tag{2.2}$$

A further inspection of [8, Ch. XII] gives the following:

Lemma 2.3. *The only isomorphism types in Lemma 2.1 which consist of self-normalising subgroups of G are the following:*

(1) D_d *for divisors* $d > 2$ *of* $(p+1)/2$ *with* $(p+1)/2d$ *odd, one class for each* d *(a subgroup* $\mathrm{D}_2 = \mathrm{V}_4$ *is never self-normalising);*
(2) D_e *for divisors* $e > 2$ *of* $(p-1)/2$ *with* $(p-1)/2e$ *odd, one class for each* e*;*
(3) $\mathrm{C}_p \rtimes \mathrm{C}_{(p-1)/2}$*, one class;*
(4) A_4 *if* $p \equiv \pm 3 \bmod (8)$*, one class;*
(5) S_4 *if* $p \equiv \pm 1 \bmod (8)$*, two classes;*
(6) A_5 *if* $p \equiv \pm 1 \bmod (5)$*, two classes.*

The subgroups of types (3), (4), (5) and (6) are maximal in G, as are the subgroups $\mathrm{D}_{(p\pm1)/2}$ in (1) and (2); the remaining subgroups listed above in (1) and (2) are self-normalising proper subgroups of $\mathrm{D}_{(p\pm1)/2}$. One of $(p \pm 1)/2$ is odd, so each of its $\delta - 1$ or $\varepsilon - 1$ divisors $d \neq 1$ or $e \neq 1$ yields a class of self-normalising dihedral subgroups. For the even integer $(p \pm 1)/2$, the proportion of its divisors which have an odd quotient is $1/(k+1)$ or $1/(l+1)$; such divisors do not include 1, and they include

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

2 if and only if $k = 1$ or $l = 1$, that is, $p \equiv \pm 5 \bmod (8)$, or equivalently $\sigma = 0$. It follows that the total number of self-normalising classes in (1) and (2) can be written as

$$\frac{\delta}{k+1} + \frac{\varepsilon}{l+1} - 2 + \sigma.$$

(Recall that one of k and l is zero, as $p \pm 1)/2$ is odd.) In addition, (3) contributes one class, (4) and (5) together contribute $\sigma + 1$, and (6) contributes 2α. Adding all these contributions we see that the total number $s(G)$ of conjugacy classes of self-normalising subgroups is given by

$$s(G) = \frac{\delta}{k+1} + \frac{\varepsilon}{l+1} + 2(\sigma + \alpha). \tag{2.3}$$

It follows that the number $n(G)$ of conjugacy classes of non-self-normalising subgroups of G is given by

$$n(G) = c(G) - s(G) = \left(2 + \frac{k-1}{k+1}\right)\delta + \left(3 + \frac{l-1}{l+1}\right)\varepsilon - 4 + \sigma. \tag{2.4}$$

Example 2.4. *Let $p = 37$. Then $(p+1)/2 = 19$, which is prime, so $\delta = 2$, and $(p-1)/2 = 18 = 2 \cdot 3^2$, so $\varepsilon = 2 \cdot 3 = 6$. We have $k = 0$ and $l = 1$. Since $p \equiv -3 \bmod (8)$ and $p \equiv 2 \bmod (5)$ we have $\sigma = \alpha = 0$.* Thus

$$i(G) = 2 \cdot 2 + 3 \cdot 6 - 3 = 19,$$
$$c(G) = 2 \cdot 2 + \frac{7}{2} \cdot 6 - 4 = 21$$

with subgroups D_3 and D_9 each forming two conjugacy classes,

$$s(G) = \frac{2}{1} + \frac{6}{2} = 5$$

represented by conjugacy classes of subgroups D_{19}, D_6, D_{18}, $\mathrm{C}_{37} \rtimes \mathrm{C}_{18}$, and A_4 (one each), and

$$n(G) = 1 \cdot 2 + 3 \cdot 6 - 4 = 16$$

represented by conjugacy classes of subgroups C_{19}, C_e ($e = 2, 3, 6, 9, 18$), D_2, D_3 (two classes), D_9 (two classes) and $\mathrm{C}_{37} \rtimes \mathrm{C}_e$ ($e = 1, 2, 3, 6, 9$). Table 1 gives similar data for the primes $p = 3, \ldots, 61$.

3. Lower bounds for the invariants

Our aim now is to find primes p for which the invariants considered above for the groups $G = \mathrm{PSL}_2(p)$ take the lowest possible values. In order to obtain uniform bounds we will assume that $p > 37$; the smaller primes can be dealt with individually, as in the preceding example (see Table 1).

We start with $i(G)$, given by (2.1). The first step is to ensure that $\sigma = \alpha = 0$ by restricting attention to primes $p \equiv \pm 3$ or $\pm 13 \bmod (40)$; Dirichlet's Theorem guarantees an infinite set of primes satisfying any one of these four congruences. It now remains to find a good upper bound on $2\delta + 3\varepsilon$, and this can be done by minimising the numbers of primes dividing $(p \pm 1)/2$. These two consecutive integers

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

TABLE 1. Invariants of $\mathrm{PSL}_2(p)$ for small primes p.

p	δ	ε	k	l	σ	α	$i(G)$	$c(G)$	$s(G)$	$n(G)$
3	1	2	0	1	0	0	3	3	1	2
5	2	2	0	1	0	0	7	7	3	4
7	3	2	2	0	1	0	10	13	5	8
11	4	2	1	0	0	1	12	14	6	8
13	2	4	0	1	0	0	13	14	4	10
17	3	4	0	3	1	0	16	20	6	14
19	4	3	1	0	0	1	15	17	7	10
23	6	2	2	0	1	0	16	21	6	15
29	4	4	0	1	0	1	18	20	8	12
31	5	4	4	0	1	1	21	27	9	18
37	2	6	0	1	0	0	19	21	5	16
41	4	6	0	2	1	1	25	31	10	21
43	4	4	1	0	0	0	17	18	6	12
47	8	2	3	0	1	0.	20	27	6	21
53	4	4	0	1	0	0	17	18	6	12
59	8	2	1	0	0	1	20	24	8	16
61	2	8	0	1	0	1	26	30	8	22

are coprime, one of them must be divisible by 2, and one of them by 3, giving four possibilities for allocating these prime factors. They are as follows, with inequalities needed to produce primes $p > 37$:

(a) $(p+1)/2 = 3s$ and $(p-1)/2 = 2r$ coprime, with $s \geq 7$ and $r \geq 10$,
(b) $(p+1)/2 = 2s$ and $(p-1)/2 = 3r$ coprime, with $s \geq 10$ and $r \geq 7$,
(c) $(p+1)/2 = 6s$ and $(p-1)/2 = r$ coprime, with $s \geq 4$ and $r \geq 19$,
(d) $(p+1)/2 = s$ and $(p-1)/2 = 6r$ coprime, with $s \geq 20$ and $r \geq 4$,

where $|G| = 12psr$ in all cases. (Remarkably, these four cases also arose recently in [12], which addressed the problem of constructing a possibly infinite set of finite simple groups of order a product of six primes.)

If in (a) or (b) we take s and r to be primes satisfying the specified inequalities and giving a prime value for p, then $\delta = \varepsilon = 4$ and so $2\delta + 3\varepsilon = 20$; moreover, $|G|$ is not divisible by 8 or by 5, so $\sigma = \alpha = 0$ and thus $i(G) = 17$. This value can also be obtained in (a) by taking $s = 9$ and $r = 13$, so that $p = 53$, but it is not hard to see that no lower value of $i(G)$ can be obtained in cases (a) to (d).

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

Thus

$$i(G) \geq 17 \tag{3.1}$$

for all G with $p > 37$, with equality whenever conditions (a) or (b) are satisfied by primes p, s and r, and also when $p = 53$. In fact, Table 1 shows that this inequality is satisfied for all $p \geq 29$, but not for any smaller primes. This proves Theorem 1.1(i).

A similar argument can be applied to $c(G)$, given by (2.2), but now we need to minimise

$$\left(2 + \frac{k}{k+1}\right)\delta + \left(3 + \frac{l}{l+1}\right)\varepsilon = \left(3 - \frac{1}{k+1}\right)\delta + \left(4 - \frac{1}{l+1}\right)\varepsilon,$$

where k and l take the values 0 and 1 in either order. Again, cases (a) and (b) achieve the minimum value for this expression, namely 22, so that

$$c(G) \geq 18 \tag{3.2}$$

for all G with $p > 37$, with the same conditions for equality as in (3.1). In this case, Table 1 shows that the bound is in fact satisfied for all $p \geq 23$, but not for $p = 19$. This proves Theorem 1.1(ii).

To minimise $s(G)$, given by (2.3), we need to minimise

$$\frac{\delta}{k+1} + \frac{\varepsilon}{l+1},$$

where again $\{k, l\} = \{0, 1\}$. This is achieved in all four cases (a) to (d) whenever one can take s and r prime. The resulting value is 6, so that

$$s(G) \geq 6 \tag{3.3}$$

for all G with $p > 37$, attained in cases (a) to (d), and thus proving Theorem 1.1(iii). However, in Example 2.4, where $p = 37$, we have $s(G) = 5$: the reason is that $(p-1)/2 = 18 = 2 \cdot 3^2$ has a repeated prime factor, so that $\varepsilon = 6$ rather than 8 which would be the case for three distinct prime factors. This explains why we have assumed here that $p > 37$.

Finally, to minimise $n(G)$ we need to minimise

$$\left(3 - \frac{2}{k+1}\right)\delta + \left(4 - \frac{2}{l+1}\right)\varepsilon.$$

Once again, cases (a) and (b) give the least value of this expression, namely 16, so that

$$n(G) \geq 16 - 4 = 12 \tag{3.4}$$

for all G such that $p > 37$, with equality as in (a) and (b). In fact, Table 1 shows that this bound is satisfied for all $p \geq 23$. This proves Theorem 1.1(iv).

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

4. **Attaining the bounds**

We have seen instances of groups G which attain the four lower bounds obtained in the preceding section, namely all the groups in cases (a) and (b) involving triples of primes p, r and s. The smallest such group in case (a) is $\mathrm{PSL}_2(29)$; however, this has $\alpha = 1$ since its order is divisible by $s = 5$, so it does not satisfy all the bounds. The next example in case (a) is $\mathrm{PSL}_2(173)$, with $r = 43$ and $s = 29$, and this has $\alpha = 0$, as required. The first example in case (b) is $\mathrm{PSL}_2(43)$, with $r = 7$ and $s = 11$. In fact, in each of cases (a) to (d) the computer searches reported in [12] found over $600,000$ instances of suitable triples of primes, all but a few having $\sigma = \alpha = 0$, so that those in cases (a) and (b) attain equality in our bounds.

Ideally, we would like infinite sets of examples attaining these bounds. In case (a) the equations

$$(p+1)/2 = 3s \quad \text{and} \quad (p-1)/2 = 2r$$

imply that $p \equiv 5 \bmod (12)$, so we can write $p = 12t + 5$ for some $t \in \mathbb{N}$. Then

$$s = (p+1)/6 = 2t+1 \quad \text{and} \quad r = (p-1)/4 = 3t+1.$$

We require p, s and r all to be prime, so we need the polynomials

$$f_i(t) = 12t+5, \quad 3t+1 \quad \text{and} \quad 2t+1 \tag{4.1}$$

representing them all to take prime values for infinitely many $t \in \mathbb{N}$.

The situation is similar in cases (b), (c) and (d): for example, in case (b) we need the polynomials

$$f_i(t) = 12t+7, \quad 3t+2 \quad \text{and} \quad 2t+1 \tag{4.2}$$

to take prime values for infinitely many $t \in \mathbb{N}$. This type of problem is the subject-matter of Schinzel's Hypothesis and the Bateman–Horn Conjecture, considered in the next section.

5. **The Bateman–Horn Conjecture**

Given a finite set of distinct polynomials $f_i(t) \in \mathbb{Z}[t]$ $(i = 1, \ldots, k)$, it is of interest to know whether they simultaneously take prime values for infinitely many $t \in \mathbb{N}$. Instances of this general problem include the following:

- the twin primes problem, with $f_1(t) = t$ and $f_2(t) = t+2$;
- the Sophie Germain primes problem, with $f_1(t) = t$ and $f_2(t) = 2t+1$;
- the Euler–Landau problem, with a single polynomial $f_1(t) = t^2 + 1$.

The following are obvious necessary conditions on the polynomials $f_i(t)$:

- they all have positive leading coefficients;
- they are all irreducible;
- their product $f(t) = f_1(t) \cdots f_k(t)$ is not identically zero modulo any prime.

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

Schinzel's Hypothesis [15], which we will abbreviate to SH, asserts that these conditions are also sufficient. This generalises earlier conjectures by Bunyakovsky [5] for $k = 1$ and by Dickson [7] where $\deg f_i = 1$ for all i. It has been proved only in the simplest case, where $k = 1$ and $\deg f_1 = 1$: this is Dirichlet's Theorem on primes in an arithmetic progression $at + b$.

Building on earlier work by Hardy and Littlewood [9] on some special cases, the Bateman–Horn Conjecture (BHC) quantifies SH by giving an estimate $E(x)$ for the number $Q(x)$ of $t \le x$ for which the values $f_i(t)$ are all prime. It asserts that

$$Q(x) \sim E(x) \quad \text{as} \quad x \to \infty$$

where

$$E(x) := C \int_a^{+\infty} \frac{dt}{\prod_i \ln f_i(t)}; \tag{5.1}$$

here C is the *Hardy–Littlewood constant*

$$C = C(f_1, \ldots, f_k) := \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\omega_f(p)}{p}\right) \tag{5.2}$$

where $\omega_f(p)$ is the number of distinct roots of the polynomial $f = f_1 \cdots f_k \bmod (p)$, and a is chosen so that the integral in (5.1) avoids any singularities, where $\ln f_i(t) = 0$ for some i.

One can regard the integral in (5.1) as a first attempt at an estimate for $Q(x)$, based on applying the Prime Number Theorem to the polynomials $f_i(t)$, on the (incorrect) assumption that they take values independently. The constant C in (5.2) can then be regarded as a product of correction factors, one for each prime p, replacing the probability $(1 - \frac{1}{p})^k$ that k randomly and independently chosen elements of $\mathbb{Z}_p$ are all non-zero with the proportion of $\mathbb{Z}_p$ where $f(t) \ne 0$.

When the three conditions of SH are satisfied the infinite product in (5.2) converges to a limit $C > 0$. Convergence is slow, but good approximations can be found by taking partial products over large initial segments of the primes. On a laptop this can take several hours, but by contrast Maple can accurately evaluate the integral in (5.1) almost instantly, by numerical integration.

Like SH, the BHC has been proved only in the simplest case, where $k = 1$ and $\deg f_1 = 1$. This is de la Vallée-Poussin's quantified form of Dirichlet's Theorem, that the primes $at + b$ are asymptotically evenly distributed among the $\varphi(a)$ congruence classes of units mod (a) (see [4, Ch. 5, §3.2], for instance).

If the conditions of SH are satisfied then $E(x) \to +\infty$ as $x \to \infty$. The BHC asserts that $Q(x) \sim E(x)$ as $x \to \infty$, so if the BHC is correct then $Q(x) \to +\infty$ also, and hence there are infinitely many $t \in \mathbb{N}$ for which each $f_i(t)$ is prime. Thus the BHC implies SH. The fact that the BHC has given impressively accurate estimates in all known applications is strong evidence that it is true, but at present there seems to be little prospect of a proof.

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

There is an interesting account in [1] of the history of the BHC, including a proof of the convergence of the product (5.2). There are shorter discussions of the BHC in [11, 12], including several applications to other problems in group theory, some involving the groups $\mathrm{PSL}_2(p)$.

Returning to our specific problem, the polynomials $f_i(t)$ in case (a), shown in (4.1), satisfy the common conditions of SH and the BHC, as do those in case (b) shown in (4.2), so if the BHC is true then in either case there are infinitely many $t \in \mathbb{N}$ with each $f_i(t)$ prime, as required. This gives a proof of Theorem 1.3 and hence (assuming the BHC) of Conjecture 1.2.

Example 5.1. *As in* [12]*, where cases (a) to (d) arose in connection with a different problem concerning the groups* $\mathrm{PSL}_2(p)$*, let* $x = 10^9$*. A computer search reported there, using the primality test within Maple, shows that in case (a) we have* $Q_a(10^9) = 614\,423$*. Evaluating* $E_a(10^9)$ *by Maple, using numerical integration, gives an estimate* $615\,580.7$*, which has a relative error of* $+0.188\%$*. Similarly, in case (b) we have* $Q_b(10^9) = 615\,369$ *and* $E_b(10^9) = 615\,580.6$*, an error of* $+0.034\%$*.*

6. Applying Heath-Brown's result

What can be proved without assuming any unproved conjectures? Heath-Brown, in an appendix to [6], has proved that there is an infinite set $\mathcal{P}$ of primes $p \equiv 5 \bmod (72)$ such that

$$\Omega(p-1) + \Omega(p+1) \le 11 \quad \text{and} \quad \Omega(p-1), \Omega(p+1) \le 8,$$

where $\Omega(n)$ is the number $\sum_{i=1}^{k} e_i$ of primes dividing an integer $n = \prod_{i=1}^{k} p_i^{e_i}$, counting repetitions. Note that if $p \in \mathcal{P}$ then $(p-1)/2$ is twice odd and $(p+1)/2$ is odd.

Let $\mathcal{G} = \{G = \mathrm{PSL}_2(p) \mid p \in \mathcal{P}\}$. If $G \in \mathcal{G}$ then since $p \equiv 5 \bmod (8)$ we have $\sigma = 0$, so (2.1) becomes

$$i(G) = 2\delta + 3\varepsilon - 3 + \alpha.$$

An upper bound (not necessarily attained) on $i(G)$ for $G \in \mathcal{G}$ is therefore obtained by taking $(p+1)/2$ and $(p-1)/2$ to be products of two and seven distinct primes, including 5 in one case, so that $\delta = 2^2 = 4$, $\varepsilon = 2^7 = 128$ and $\alpha = 1$. This gives an upper bound

$$i(G) \le 2 \times 4 + 3 \times 128 - 3 + 1 = 390$$

for all $G \in \mathcal{G}$.

Since $p \equiv 5 \bmod (8)$ we have $k = 0$ and $l = 1$, so (2.2) becomes

$$c(G) = 2\delta + \frac{7}{2}\varepsilon - 4 + 2\alpha.$$

The same assumptions as before on the primes dividing $(p \pm 1)/2$ therefore give an upper bound

$$c(G) \le 2 \times 4 + \frac{5}{2} \times 128 - 4 + 2 = 454$$

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

for all $G \in \mathcal{G}$. Since $k = 0$, $l = 1$ and $\sigma = 0$, (2.3) becomes

$$s(G) = \delta + \frac{1}{2}\varepsilon + 2\alpha.$$

With this changed weighting for δ and ε, an upper bound for $s(G)$ is now obtained by assigning seven distinct prime factors to $(p+1)/2$ and two to $(p-1)/2$, again including 5, so that $\delta = 128$, $\varepsilon = 4$ and $\alpha = 1$, giving an upper bound

$$s(G) \leq 128 + \frac{1}{2} \times 4 + 2 = 132$$

for all $G \in \mathcal{G}$. Finally (2.4) becomes

$$n(G) = \delta + 3\varepsilon - 4,$$

so the same assignment of prime factors as for $i(G)$ and $c(G)$ gives an upper bound

$$n(G) \leq 4 + 3 \times 128 - 4 = 384$$

for all $G \in \mathcal{G}$. This completes the proof of Theorem 1.4.

Acknowledgments

The author is grateful to Mark Lewis for the seminar which inspired this work, to Natalia Maslova for organising the workshop in which it took place, and to Alexander Zvonkin for some very helpful remarks on this paper and for the computations reported in [12] and used again here.

References

[1] S. L. Aletheia-Zomlefer, L. Fukshansky and S. R. Garcia, The Bateman–Horn conjecture: heuristics, history, and applications, *Expo. Math.*, **38** no. 4 (2020) 430–479.

[2] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.*, **16** (1962) 363–367.

[3] M. Bianchi, R. D. Camina, M. L. Lewis, E. Pacifici and L. Sanus, On non self-normalizing subgroups, *Springer Proc. Math. Statistics (Group Theory, Ischia, 2024)*, to appear; see also arxiv.math[GR]: 2411.18102.

[4] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Translated from the Russian by Newcomb Greenleaf, Pure and Applied Mathematics, **20**, Academic Press, New York-London, 1966.

[5] V. Bouniakowsky, Sur les diviseurs numériques invariables des fonctions rationnelles entières, *Mém. Acad. Sci. St. Péteresbourg*, 6^{e} série, **VI** (1857) 305–329. Available at: https://books.google.fr/books?hl=fr&id=wXIhAQAAMAAJ&pg=PA305#v=onepage&q&f=false.

[6] T. C. Burness, M. W. Liebeck and A. Shalev, On the length and depth of finite groups, *Proc. London Math. Soc. (3)*, **119** no. 6 (2019) 1464–1492.

[7] L. E. Dickson, A new extension of Dirichlet's theorem on prime numbers, *Messenger of Math.*, **33** (1904) 155–161.

[8] L. E. Dickson, *Linear groups*, Dover Publications, Inc., New York, 1958.

https://dx.doi.org/10.22108/ijgt.2025.144154.1942

[9] G. H. Hardy and J. E. Littlewood, Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.*, **44** no. 1 (1923) 1–70.

[10] B. Huppert, *Endliche Gruppen I* (2nd ed.), Springer-Verlag, Berlin - Heidelberg - New York, 1979.

[11] G. A. Jones and A. K. Zvonkin, Groups of prime degree and the Bateman–Horn Conjecture, *Expo. Math.*, **41** no. 1 (2023) 1–19.

[12] G. A. Jones and A. K. Zvonkin, Orders of simple groups and the Bateman–Horn conjecture, *Int. J. Group Theory*, **13** no. 3 (2024) 257–269.

[13] W. J. LeVeque, *Fundamentals of number theory*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1977.

[14] M. Lewis, On self-normalizing subgroups (online seminar), Ural Workshop on Group Theory and Combinatorics, Yekaterinburg, 2024. http://uwgtc.imm.uran.ru.

[15] A. Schinzel and W. Sierpiński, Sur certaines hypothèses concernant les premiers, (French) *Acta Arith.*, **4** (1958) 185–298; erratum, **5** (1958) 259.

Gareth A. Jones

School of Mathematical Sciences, University of Southampton, Southampton SO17 1BJ, UK

Email: G.A.Jones@maths.soton.ac.uk

https://dx.doi.org/10.22108/ijgt.2025.144154.1942