ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 41, Number 5, 2011

NCF-DISTINGUISHABLITY BY PRIME GRAPH OF $\mathbf{PGL(2,p)}$ WHERE p IS A PRIME

M. KHATAMI, B. KHOSRAVI AND Z. AKHLAGHI

ABSTRACT. Let G be a finite group. The prime graph $\Gamma(G)$ of G is defined as follows. The vertices of $\Gamma(G)$ are the primes dividing the order of G and two distinct vertices p, p' are joined by an edge if there is an element in G of order pp'. Let p be a prime number. In [**4**], the authors determined the structure of finite groups with the same element orders as $PGL(2,p)$, and it is proved that there are infinitely many nonisomorphic finite groups with the same element orders as $PGL(2,p)$. Therefore there are infinitely many nonisomorphic finite groups with the same prime graph as $PGL(2,p)$.

We know that $PGL(2,p)$ has a unique nonabelian composition factor which is isomorphic to $PSL(2,p)$. Let p be a prime number which is not a Mersenne or Fermat prime and $p \neq 11$, 19. In this paper we determine the structure of finite groups with the same prime graph as $PGL(2,p)$ and as the main result we prove that if G is a finite group such that $\Gamma(G) = \Gamma(PGL(2,p))$ and $p \neq 13$, then G has a unique nonabelian composition factor which is isomorphic to $PSL(2,p)$ and if $p = 13$, then G has a unique nonabelian composition factor which is isomorphic to $PSL(2,13)$ or $PSL(2,27)$.

1. Introduction. If n is an integer, then we denote by $\pi(n)$ the set of all prime divisors of n. Let G be a finite group. Denote by $\pi(G)$ the set of primes p such that G contains an element of order p. Also the set of orders of elements of G is denoted by $\pi_e(G)$. This set is closed under divisibility and is uniquely determined by the set $\mu(G)$ of elements in $\pi_e(G)$ which are maximal under the divisibility relation. We denote by $h(G)$, the number of pairwise non-isomorphic groups H with $\pi_e(G) = \pi_e(H)$. The prime graph $\Gamma(G)$ of a group G is defined as a graph with vertex set $\pi(G)$ in which two distinct primes $p, p' \in \pi(G)$ are adjacent if G contains an element of order pp'. Let $t(G)$ be the number

2010 AMS *Mathematics subject classification.* Primary 20D05, 20D60, 20D08.
Keywords and phrases. Prime graph, simple group, composition factors, linear group.
Received by the editors on July 19, 2008, and in revised form on January 19, 2009.
DOI:10.1216/RMJ-2011-41-5-1523

of connected components of $\Gamma(G)$ and $\pi_1, \pi_2, \dots, \pi_{t(G)}$ the connected components of $\Gamma(G)$. If $2 \in \pi(G)$, then we always suppose that $2 \in \pi_1$. Then π_1 is called the even component of $\Gamma(G)$ and $\pi_2, \dots, \pi_{t(G)}$ are called the odd components of $\Gamma(G)$. Let m and n be positive integers. We write $m \sim n$, if every prime divisor of m is adjacent to every prime divisor of n. There are many results about the prime graph of a finite group [**21**].

Hagie in [**8**] determined finite groups G satisfying $\Gamma(G) = \Gamma(S)$, where S is a sporadic simple group. It is proved that if $q = 3^{2n+1}$ $(n > 0)$, then the simple group ${}^2G_2(q)$ is uniquely determined by its prime graph [**3, 33**]. A group G is called a CIT group if G is of even order and the centralizer in G of any involution is a 2-group. In [**15**] finite groups with the same prime graph as a CIT simple group are determined. Also in [**16**] it is proved that if $p > 11$ is a prime number and $p \not\equiv 1 \pmod{12}$, then $PSL(2,p)$ is uniquely determined by its prime graph. In [**13, 14, 19**], finite groups with the same prime graph as $PSL(2,q)$ are determined. In [**1**], the authors determined finite groups with the same prime graph as ${}^2F_4(q)$, where $q = 2^{2n+1} > 2$. We introduce the following definition.

Definition 1.1. A finite group G is called *nonabelian composition factor(s) distinguishable by prime graph* (briefly, NCF-distinguishable by prime graph) if every finite group H with $\Gamma(H) = \Gamma(G)$ has the same nonabelian composition factor(s) as G.

In [**4**], it is proved that if $q = p^\alpha$, where p is a prime and $\alpha > 1$, then $PGL(2,q)$ is uniquely determined by its element orders. Also in [**26**], it is proved that there are infinitely many nonisomophic finite groups with the same element orders as $PGL(2,p)$. Obviously these groups have the same prime graph as $PGL(2,p)$. We know that $PGL(2,p)$ has a unique nonabelian composition factor which is isomorphic to $PSL(2,p)$. In this paper as the main result we prove the following theorem:

Main theorem. *Let G be a finite group, and let p be a prime number such that $\Gamma(G) = \Gamma(PGL(2,p))$, where $p \neq 11$, 19 and p is not a Mersenne or Fermat prime.*

(a) *If $p \neq 13$, then G has a normal series $1 \trianglelefteq N \trianglelefteq N.P \trianglelefteq N.P.A = G$, such that N is a nilpotent group, $P \cong PSL(2,p)$, $A \leq \mathbf{Z}_2$ and*

$\pi(N) \subseteq \pi(p-1)$. If $|N|$ is odd and $p \equiv 5,\ 11 \pmod{12}$, then $N = 1$. Thus $PGL(2,p)$ is NCF-distinguishable by prime graph.

(b) *If $p = 13$, then G has a normal series $1 \trianglelefteq N \trianglelefteq N.P \trianglelefteq N.P.A = G$, such that $P \cong PSL(2,13)$ and N is a 2-group; or $P \cong PSL(2,27)$ and N is a 3-group, and $A \leq Out(P)$.*

By using the classification of finite simple groups, the structure of a finite group G such that its prime graph is not connected has been determined by Gruenberg and Kegel, in an unpublished paper. Later, Williams published this result together with a classification of finite simple groups with a disconnected prime graph, which are distinct from Lie-type groups of even characteristic, see [**32**]. In [**9**], a similar description was given for simple Lie-type groups in an even characteristic. The connected components of the prime graph of non-abelian simple groups with disconnected prime graph are listed in [**22**] and throughout this paper we use this list.

Throughout this paper, all groups are finite and by simple groups we mean non-abelian simple groups. All further unexplained notations are standard and refer to [**5**]. We use the results of Williams [**32**], Iiyori and Yamaki [**9**] and Kondrat'ev [**20**] about the prime graph of simple groups. We denote by (a,b) the greatest common divisor of positive integers a and b. Let m be a positive integer and p be a prime number. Then $|m|_p$ denotes the $p-$part of m. In other words, $|m|_p = p^k$ if $p^k \mid m$ but $p^{k+1} \nmid m$.

2. Preliminary results.

Remark 2.1. First we give a brief description of the prime graph of $PGL(2,p)$, where p is an odd prime. By [**4**], it follows that

$$\mu(PGL(2,p)) = \{p, p-1, p+1\}.$$

Therefore, by assumption, the prime graph of $PGL(2,p)$ has two connected components. We note that $\{p\}$ is an odd component of the prime graph which is a singleton (a connected component consist of one vertex) and p is the greatest prime divisor of $|PGL(2,p)|$.

It is sometimes convenient to represent the graph $\Gamma(G)$ in a compact form. By the compact form we mean a graph whose vertices are

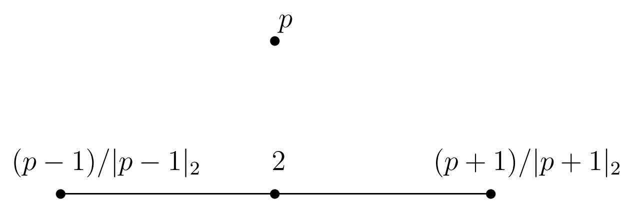

FIGURE 1.

labeled with pairwise coprime natural numbers. A vertex labeled n represents the complete subgraph of $\Gamma(G)$ with vertex set $\pi(n)$. An edge connecting n and m represents the set of edges of $\Gamma(G)$ that connect each vertex in $\pi(n)$ with each vertex in $\pi(m)$. Figure 1 depicts the compact form of the prime graph of $PGL(2,p)$, where p is an odd prime and p is not a Fermat prime or a Mersenne prime.

Remark 2.2. If $\Gamma(PGL(2,p))$ has two complete components, then we have $\pi(p-1)=\{2\}$ or $\pi(p+1)=\{2\}$, which implies that p is a Fermat or Mersenne prime.

Lemma 2.3 (see [**24, 25, 32**]). *A finite group G with disconnected prime graph $\Gamma(G)$ satisfies one of the following conditions*:

(a) *$t(G)=2$ and $G=KC$ is a Frobenius group with kernel K and complement C and two connected components of $\Gamma(G)$ are $\Gamma(K)$ and $\Gamma(C)$. Moreover K is nilpotent, and hence $\Gamma(K)$ is a complete graph. If C is solvable, then $\Gamma(C)$ is complete*; *otherwise, $\{2,3,5\}\subseteq\pi(G)$ and $\Gamma(C)$ can be obtained from the complete graph with vertex set $\pi(C)$ by removing the edge $\{3,5\}$.*

(b) *$t(G)=2$ and G is a 2-Frobenius group, i.e., $G=ABC$, where A and AB are normal subgroups of G, B is a normal subgroup of BC, and AB and BC are Frobenius groups. The two connected components of $\Gamma(G)$ are complete graphs $\Gamma(AC)$ and $\Gamma(B)$.*

(c) *G is an extension of a nilpotent group N which is trivial or a $\pi_1(G)-$group, by a group of the form $P.A$, where $P\leq P.A\leq \mathrm{Aut}\,(P)$*

for some non-abelian simple group P with disconnected $\Gamma(P)$, and $A = 1$ or A is a $\pi_1(G)-$group. Moreover, $t(P) \geq t(G)$.

Lemma 2.4 (see [**23**, Lemma 1]). *Let N be a normal subgroup of G. Assume that G/N is a Frobenius group with Frobenius kernel F and cyclic Frobenius complement C. If $(|N|, |F|) = 1$, and F is not contained in $NC_G(N)/N$, then $p|C| \in \pi_e(G)$, where p is a prime factor of $|N|$.*

Lemma 2.5 (see [**23**]). *Let G be a finite group having a non-trivial solvable normal subgroup. Then $h(G) = \infty$.*

Lemma 2.6. *Let $L = L_2(p)$, where p is a prime, $p > 3$.*

(a) (see [**3**]). *L has an irreducible module V over $\mathbf{C}$ of degree $p-1$ such that all elements of order p in L act on V fixed-point-freely and an element of order $(p+1)/2$ has a fixed point in V.*

(b) (see [**2**]). *Let W be a reduction of V modulo 2. If $(p-1)/2$ is odd, then there exists a non-split extension E of W by L.*

Lemma 2.7 (see [**4**]). *Suppose that $p > 3$ is a prime number. Then there exists an extension E of the $L_2(p)$-module W from Lemma 2.6 by $L = L_2(p)$ with $\pi_e(E) = \pi_e(\mathrm{PGL}\,(2,p))$.*

Lemma 2.8 (see [**29**, Proposition 3.2]). *Let G be a finite group and H a normal subgroup of G. Suppose G/H is isomorphic to $PSL(2,q)$, q odd and $q > 5$, and that an element t of order 3 in $G \setminus H$ has no fixed points on H. Then $H = 1$.*

Lemma 2.9 (see [**4**]). *Let $M^1 = A_2(q)$ and $M^{-1} = {}^2A_2(q)$, where $q = p_0^\beta$ and p_0 is a prime, $\beta > 0$. Then for $\varepsilon = \pm 1$,*

$$\mu(M^\varepsilon) = \left\{q-\varepsilon, \frac{p_0(q-\varepsilon)}{(3,q-\varepsilon)}, \frac{(q^2-1)}{(3,q-\varepsilon)}, \frac{q^2+\varepsilon q+1}{(3,q-\varepsilon)}\right\}, \text{ if } q \text{ is odd.}$$

$$\mu(M^\varepsilon) = \left\{q-\varepsilon, \frac{2(q-\varepsilon)}{(3,q-\varepsilon)}, \frac{q^2-1}{(3,q-\varepsilon)}, \frac{q^2+\varepsilon q+1}{(3,q-\varepsilon)}, 4\right\}, \text{ if } q \text{ is even.}$$

The following lemma is a consequence of Proposition 3.1 in [**31**].

Lemma 2.10. *For a positive integer m, let*

$$\nu(m) = \begin{cases} m & m \equiv 0 \pmod 4 \\ m/2 & m \equiv 2 \pmod 4 \\ 2m & m \equiv 1 \pmod 2. \end{cases}$$

Let $q = p^\alpha$, and let r be an odd prime such that $p \neq r$.

(a) *If $G = A_{n-1}(q)$ and $\mathrm{ord}_r q \leq n-2$, then $r \sim p$ in $\Gamma(G)$.*

(b) *If $G = {}^2A_{n-1}(q)$ and $\nu(\mathrm{ord}_r q) \leq n-2$, then $r \sim p$ in $\Gamma(G)$.*

Lemma 2.11 (see [**27**]). *Let G be a finite group and N a nontrivial normal $p-$subgroup, for some prime p, and set $K = G/N$. Suppose that K contains an element x of order m coprime to p such that $\langle \phi|_{\langle x \rangle}, 1|_{\langle x \rangle} \rangle > 0$ for every Brauer character ϕ of (an absolutely irreducible representation of) K in characteristic p. Then G contains elements of order pm.*

Lemma 2.12 (see [**7**, Theorem 4.7]). *Let F be a field of order p^k, and let $\rho \in \mathbf{C}$ be a (p^k-1)th root of unity, $\sigma \in \mathbf{C}$ a (p^k+1)th root of unity, $z = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $a = \left(\begin{smallmatrix} \nu & 0 \\ 0 & -\nu \end{smallmatrix}\right)$, $d = \left(\begin{smallmatrix} 1 & 0 \\ \nu & 1 \end{smallmatrix}\right)$, where ν is a generator of the cyclic multiplicative group F^*, $c = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and b be an element of order p^k+1 in $SL(2,p^k)$. Then for $p^k \equiv 1 \pmod 4$ the ordinary character table of $PSL(2,p^k)$ is* (*as shown in Table* 2.1).

TABLE 2.1.

	$\langle z \rangle$	$\langle z \rangle c$	$\langle z \rangle d$	$\langle z \rangle a^l$	$\langle z \rangle a^{(p^k-1)/4}$	$\langle z \rangle b^m$
1_G	1	1	1	1	1	1
ψ	p^k	0	0	1	1	-1
χ_i	p^k+1	1	1	$\rho^{il}+\rho^{-il}$	$\rho^{i(p^k-1)/4}+\rho^{-i(p^k-1)/4}$	0
θ_j	p^k-1	-1	-1	0	0	$-\sigma^{jm}-\sigma^{-jm}$
ξ_1	$(p^k+1)/2$	$(1+\sqrt{p^k})/2$	$(-1-\sqrt{-p^k})/2$	$(-1)^l$	$(-1)^{(p^k-1)/4}$	0
ξ_2	$(p^k+1)/2$	$(1-\sqrt{p^k})/2$	$(1+\sqrt{p^k})/2$	$(-1)^l$	$(-1)^{(p^k-1)/4}$	0

where $i = 2,4,6,\ldots,(p^k-5)/2$, $j = 2,4,6,\ldots,(p^k-1)/2$, $1 \leq l \leq (p^k-5)/4$ and $1 \leq m \leq (p^k-1)/4$.

For $p^k \equiv -1 \pmod 4$ the ordinary character table of $PSL(2,p^k)$ is (as shown in Table 2.2).

TABLE 2.2.

	$\langle z\rangle$	$\langle z\rangle c$	$\langle z\rangle d$	$\langle z\rangle a^l$	$\langle z\rangle b^m$	$\langle z\rangle b^{\frac{p^k+1}{4}}$
1_G	1	1	1	1	1	1
ψ	p^k	0	0	1	-1	-1
χ_i	p^k+1	1	1	$\rho^{il}+\rho^{-il}$	0	0
θ_j	p^k-1	-1	-1	0	$-\sigma^{jm}-\sigma^{-jm}$	$-\delta^{j\frac{p^k+1}{4}}-\delta^{-j\frac{p^k+1}{4}}$
η_1	$\frac{p^k-1}{2}$	$\frac{-1+\sqrt{-p^k}}{2}$	$\frac{-1-\sqrt{-p^k}}{2}$	0	$(-1)^{m+1}$	$(-1)^{\frac{p^k+1}{4}+1}$
η_2	$\frac{p^k-1}{2}$	$\frac{-1-\sqrt{-p^k}}{2}$	$\frac{-1+\sqrt{-p^k}}{2}$	0	$(-1)^{m+1}$	$(-1)^{\frac{p^k+1}{4}+1}$

where $i = 2, 4, 6, \ldots, (p^k-3)/2$, $j = 2, 4, 6, \ldots, (p^k-3)/2$, $1 \le l \le (p^k-3)/4$ and $1 \le m \le (p^k-3)/4$.

Remark 2.13. We note that if $(3^\beta - 1)/2$ is a prime number, then β is an odd prime. Also if $(3^\beta + 1)/2$ is a prime number, then β is a power of 2.

Lemma 2.14 (see [**28**, page 29]). *Let $a > 1$, m and n be positive integers. Then*

$$(a^n-1, a^m-1) = a^{(n,m)} - 1.$$

Lemma 2.15 (see [**6**, Remark 1]). *The equation $p^m - q^n = 1$, where p and q are primes and $m, n > 1$ has only one solution, namely $3^2 - 2^3 = 1$.*

Lemma 2.16 (see [**17**]). *Let n and q be positive integers. If q is odd, then $|(q^{2n}-1)/(q^2-1)|_2 = |n|_2$.*

Lemma 2.17 (see [**6**]). *With the exceptions of the relations $(239)^2 - 2(13)^4 = -1$ and $3^5 - 2(11)^2 = 1$, every solution of the equation*

$$p^m - 2q^n = \pm 1; \quad p,\ q \text{ prime; } m, n > 1$$

has exponents $m = n = 2$; i.e. it comes from a unit $p - q.2^{1/2}$ of the quadratic field $Q(2^{1/2})$ for which the coefficients p and q are primes.

Lemma 2.18 (Zsigmondy theorem) (see [**34**]). *Let p be a prime, and let n be a positive integer. Then one of the following holds*:

(i) *there is a primitive prime p' for $p^n - 1$, that is, $p' \mid (p^n - 1)$ but $p' \nmid (p^m - 1)$, for every $1 \leq m < n$,*

(ii) *$p = 2$, $n = 1$ or 6,*

(iii) *p is a Mersenne prime and $n = 2$.*

In the sequel we recall the concept of quadratic residue and the Legendre symbol from number theory.

Remark 2.19 (see [**28**]). Let $(k, n) = 1$. If there is an integer x such that $x^2 \equiv k \pmod{n}$, then k is called a *quadratic residue* $\pmod{n}$. Otherwise k is called a *quadratic nonresidue* $\pmod{n}$.

Let p be an odd prime. The symbol (a/p) will have the value 1 if a is a quadratic residue $\pmod{p}$, -1 if a is a quadratic nonresidue $\pmod{p}$, and zero if $p \mid a$. The symbol (a/p) is called the *Legendre symbol.*

Let p be a prime number and $(a, p) = 1$. Let $k \geq 1$ be the smallest positive integer such that $a^k \equiv 1 \pmod{p}$. Then k is called *the order of a with respect to p* and we denote it by $\mathrm{ord}_p(a)$. Obviously by Fermat's little theorem it follows that $\mathrm{ord}_p(a) \mid (p-1)$. Also if $a^n \equiv 1 \pmod{p}$, then $\mathrm{ord}_p(a) \mid n$. Similarly if $q = p^\alpha$, then $\mathrm{ord}_q a$ is defined.

Lemma 2.20 (see [**28**]). *Let p be an odd prime. Then $(-1/p) = (-1)^{(p-1)/2}$.*

3. Proof of the main theorem. We note that if G is a group such that $\Gamma(G) = \Gamma(PGL(2,2))$, then $|G| = 2^a 3^b$, for some integers a and b, and so G is solvable. Therefore G does not have any non-abelian composition factor. Also we know that $PGL(2,2)$ does not have any non-abelian composition factor, and so $PGL(2,2)$ is NCF-distinguishable. Therefore in this section we suppose that p is an odd prime.

Lemma 3.1. *Let G be a group such that $\Gamma(G) = \Gamma(PGL(2,p))$, where p is a prime. If p is not a Fermat or Mersenne prime and $p \neq 11$, 19, then G is neither a Frobenius group nor a 2-Frobenius group.*

Proof. If G is a 2-Frobenius group, then by Lemma 2.3, the graph components of $\Gamma(G)$ are complete. So by Remark 2.2, p is a Mersenne or Fermet prime, which is a contradiction.

If G is a Frobenius group, then by Lemma 2.3, either the graph components of $\Gamma(G)$ are complete, which is a contradiction, or $\{2,3,5\} \subseteq \pi(G)$ and $\Gamma(C)$ can be obtained from the complete graph with vertex set $\pi(C)$ by removing the edge $\{3,5\}$. So we have $\pi(p-1) = \{2,3\}$ and $\pi(p+1) = \{2,5\}$; or $\pi(p-1) = \{2,5\}$ and $\pi(p+1) = \{2,3\}$. If $p-1 = 2^{\alpha}3^{\beta}$ and $p+1 = 2^{a}5^{b}$, for some non negative integers α, β, a and b, then $2^{\alpha}3^{\beta}+2 = 2^{a}5^{b}$. Therefore $a=1$ or $\alpha=1$. If $a=1$ and p_0 is a primitive prime of $5^{b}-1$, then $p_0 = 2$ or $p_0 = 3$. If $p_0 = 2$, then $b=1$ and $p=9$, which is impossible. If $p_0 = 3$, then $b=2$ and $p=49$, which is a contradiction. Let $\alpha = 1$. Then by Lemma 2.18, either $\beta = 1$, which implies that $p=7$ and this is excluded, or $3^{2\beta}-1$ has a primitive prime, say p_0. Then $p_0 = 5$ and hence $\beta = 2$ and $p = 19$, which is a contradiction. If $p-1 = 2^{\alpha}5^{\beta}$ and $p+1 = 2^{a}3^{b}$, for some non negative integers α, β, a and b, then similarly we conclude that $p = 11$ and we get a contradiction. □

Proof of the main theorem. By Lemmas 2.3 and 3.1, G is an extension of a nilpotent group N which is trivial or a π_1-group, by a group of the form $P.A$, where $P \leq P.A \leq \mathrm{Aut}\,(P)$ for some non-abelian simple group P with disconnected $\Gamma(P)$, and $A=1$ or A is a π_1-group. Moreover, $t(P) \geq t(G)$. Now using the classification of finite simple groups and the results in Tables 1–3 in [**22**], we consider the following cases.

Case 1. Let $P \cong A_{p'}$, $A_{p'+1}$ or $A_{p'+2}$, where $p' \geq 5$ is an odd prime. Since $\{p'\}$ is an odd component of P, by Remark 2.1 it follows that $p = p'$ and

$$\pi((p-1)!) \subseteq \pi(p^2-1) = \pi_1(PGL(2,p)).$$

If $x \mid (p-2)$, then $x \mid (p^2-1)$, which implies that $x=3$, and so there exists a natural number t such that $p-2 = 3^t$. If $x \mid (p-3)$, then $x \mid (p^2-1)$, which implies that $x=2$, and so there exists a natural number r such that $p-3 = 2^r$. Therefore $3^t - 2^r = 1$, and so we have either $(t,r) = (2,3)$, or $t=r=1$. If $(t,r) = (2,3)$, it follows that $p = 11$, which is a contradiction. If $r=t=1$, then $p=5$, which is a Fermat prime and this is impossible.

Case 2. Let $P \cong A_{p'-1}(q)$, where $q = p_0^{\beta}$ and $(p',q) \neq (3,2),(3,4)$. Then similarly to the above case we have

$$\pi_1(P) = \pi\Big(q^{p'(p'-1)/2}\prod_{i=1}^{p'-1}(q^i-1)\Big) \subseteq \pi(p^2-1), \tag{1}$$

$$\frac{q^{p'}-1}{(q-1)(p',q-1)} = p^{\alpha}, \text{ for some } \alpha > 0.$$

(a) Let $p' = 3$. So $(q^2+q+1)/(3,q-1) = p^{\alpha}$. We have the following subcases.

(a.1) Let $(3,q-1) = 3$. Therefore $q(q+1) = 3p^{\alpha} - 1$ and so $p_0 \mid (3p^{\alpha}-1)$. On the other hand, $p_0 \mid (p^2-1)$, by (1). So $p_0 \mid (p^{2\alpha}-1)$, which implies that $p_0 = 2$. Let $x \in \pi(q+1)$. Therefore $x \mid (3p^{\alpha}-1)$. Also by (1), $x \mid (p^{2\alpha}-1)$, which implies that $x = 2$, and this is a contradiction, since $q+1$ is odd.

(a.2) Let $(3,q-1) = 1$. So $q(q+1) = p^{\alpha} - 1$. By Lemma 2.18, $p^{\alpha}-1$ has a primitive prime, say x. By (1), $x \mid (p^2-1)$, which implies that $\alpha = 1$ or $\alpha = 2$. Let $\alpha = 2$. Therefore $q(q+1) = p^2 - 1$ and by (1), $\pi(q(q+1)(q-1)) \subseteq \pi(p^2-1)$. If $y \in \pi(q-1)$, then $y \mid (p^2-1)$. Hence $y \mid (q+1)$ and so $y = 2$. Thus q is a Fermat prime, and so $q = p_0$ and $p_0(p_0+1) = p^2 - 1$. If $p_0 \mid (p-1)$, then there is a natural number h such that $hp_0 = p-1$ and $h(p+1) = p_0+1$. Therefore $h(hp_0+2) = p_0+1$, which implies that $hp_0+2 \leq p_0+1$, and this is a contradiction. Therefore $p_0 \mid (p+1)$ and we conclude that there is a natural number h such that $hp_0 = p+1$. Since $p_0(p_0+1) = p^2-1$, it follows that $h(p-1) = p_0+1$. Therefore $p_0(h^2-1) = 2h+1$ and hence $h^2-1 < 2h+1$. Thus $h \leq 2$, which is a contradiction. Therefore $\alpha = 1$. Hence $p-1 = q(q+1)$. Let $x \in \pi(q-1)$. By (1), $x \mid (p^2-1)$. If $x \mid (p-1)$, then $x = 2$, since $p-1 = q(q+1)$. If $x \mid (p+1)$, then $x \mid (q^2+q+2)$, which implies that $x \mid (q+3)$, and hence $x = 2$. So q is a Fermat prime and $q = p_0$. By Lemma 2.9 and our assumptions, we have

$$\mu(A_2(p_0)) = \{p_0(p_0-1), p_0^2-1, p_0^2+p_0+1\}. \tag{2}$$

If there exists $2 \neq s \in \pi(p_0+1)$, then we have $s \nsim p_0$ in $\Gamma(A_2(p_0))$. On the other hand, $p_0(p_0+1) = p-1$, and so $p_0 \in \pi(p-1)$ and $\pi(p_0+1) \subseteq \pi(p-1)$. Also we know that $p-1 \in \mu(PGL(2,p))$ and so every two prime divisors of $p-1$ are joined to each other, and $|A| \mid 2$, since by Lemma 2.3, $A \leq Out(P)$. It follows that $p_0 \in \pi(N)$ or $s \in \pi(N)$. Since p is not a Mersenne prime there exists $2 \neq r \in \pi(p+1)$. Since $\pi_1(P) = \pi(p_0(p_0^2-1))$ and $p_0(p_0+1) = p-1$ and $\pi(p_0-1) = \{2\}$, we conclude that $\pi_1(P) \cap \pi(p+1) = \{2\}$. Also $|A| \mid 2$, which implies that $r \in \pi(N)$. So $r \sim p_0$ or $r \sim s$, since N is nilpotent, which is a contradiction by Figure 1.

If $\pi(p_0+1) = \{2\}$, then $p_0 = 3$, since p_0 is a Fermat prime. Thus we have $p = 13$. We note that $7 \in \pi(PGL(2,13))$ and $7 \notin \pi(A_2(3))$ and $|A| \mid 2$. Therefore $7 \in \pi(N)$. Let $x \in P$, $X = \langle x \rangle$ and $o(x) = 3$. Now by using [**30**], about irreducible characters of $A_2(3) \pmod 7$, we can see that

$$\begin{aligned}
\langle 1|_X, 1|_X \rangle &= 1;\\
\langle 12|_X, 1|_X \rangle &= \frac{1}{3}(12 + 2\times 3) = 6;\\
\langle 13|_X, 1|_X \rangle &= \frac{1}{3}(13 + 2\times 4) = 7;\\
\langle 16_1|_X, 1|_X \rangle &= \langle 16_2|_X, 1|_X \rangle = \langle 16_3|_X, 1|_X \rangle = \langle 16_4|_X, 1|_X \rangle\\
&= \frac{1}{3}(16 + 2\times(-2)) = 4;\\
\langle 26_1|_X, 1|_X \rangle &= \langle 26_2|_X, 1|_X \rangle = \langle 26_3|_X, 1|_X \rangle\\
&= \frac{1}{3}(26 + 2\times(-1)) = 8;\\
\langle 27|_X, 1|_X \rangle &= \frac{1}{3}(27 + 2\times 0) = 9;\\
\langle 39|_X, 1|_X \rangle &= \frac{1}{3}(39 + 2\times 3) = 15.
\end{aligned}$$

Therefore, for every irreducible character ϕ of $A_2(3) \pmod 7$, we show that

$$\langle \phi|_X, 1|_X \rangle = \frac{1}{|X|}\sum_{x\in X}\phi(x) > 0.$$

Now by using Lemma 2.11, it follows that $3 \sim 7$ in $\Gamma(G)$, which is a contradiction.

(b) Let $p' \geq 5$. By [**31**], the order of a maximal torus of $A_{p'-1}(q)$ is in the form of $(\prod_{i=1}^{t}(q^{k_i}-1))/((p', q-1)(q-1))$, where $p' = \sum_{i=1}^{t} k_i$. Since the graph of every maximal torus T is complete, it follows that $\pi(T) \subseteq \pi(p-1)$ or $\pi(T) \subseteq \pi(p+1)$. We consider the following subcases:

(b.1) Let $p_0 \neq 2$. By Lemma 2.10, every prime divisor of $q^i - 1$, where $1 \leq i \leq p'-2$ is adjacent to p_0. Since $p'-1$ is even, it follows that $q^{p'-1} - 1 = (q^{(p'-1)/2} - 1)(q^{(p'-1)/2} + 1)$. If $\pi(q^{(p'-1)/2} - 1) = \{2\}$, then

$(q,p')=(3,5)$, which implies that $p=11$, and this is a contradiction. If $p' \mid (q-1)$ and $\pi((q^{(p'-1)/2}-1)/p')=\{2\}$, then $p'=5$ and q is a Mersenne prime. Therefore $q^2-1=2^t.5$, for some integer t, which implies that $q=11$ and we get a contradiction. So there exists $2\neq r\in\pi((q^{(p'-1)/2}-1)/(p',q-1))$. Since $2\leq(p'-1)/2\leq p'-2$, we have $r\sim p_0$ in $\Gamma(G)$, by the above discussion. Thus $\pi_1(P)\subseteq\pi(p-1)$ or $\pi_1(P)\subseteq\pi(p+1)$. Let $\pi_1(P)\subseteq\pi(p+\varepsilon)$, where $\varepsilon=\pm1$. Since $A\leq Out(P)$, we conclude that $\pi(A)\subseteq\pi(\beta)\cup\{2,(p',q-1)\}$. If $(p',q-1)=p'$, then $p'\in\pi(p+\varepsilon)$, and so $p'\notin\pi(p-\varepsilon)$. If $2\neq s\in\pi(\beta)\cap\pi(p-\varepsilon)$, then $s\sim p_0$ in $\Gamma(G)$, since s is the order of a field automorphism and so $s\sim\pi(A_{p'-1}(p_0))$. So we get a contradiction, since $p_0\in\pi(p+\varepsilon)$. Therefore $\pi(A)\cap\pi(p-\varepsilon)=\{2\}$. By the above discussion $\pi(p-\varepsilon)\setminus\{2\}\subseteq\pi(N)$.

Let x be a primitive prime of $p_0^{\beta(p'-2)}-1$ and let y be a primitive prime of $p_0^{\beta(p'-1)}-1$. We note that $y\not\sim x$, since otherwise $(q^{p'-2}-1)(q^{p'-1}-1)$ divides the order of a maximal torus of P and so $p'-1+p'-2\leq p'$, which implies that $p'\leq 3$, and this is a contradiction. Let $x\in\pi(A)$. If $(q-1,p')=p'$ and $x=p'$, then $x\mid(q-1)$ and so $p'-2=1$, which is a contradiction. Since x is a primitive prime of $q^{p'-2}-1$, it follows that $\beta(p'-2)\leq x-1$. Therefore $x\notin\pi(\beta)$ and so we conclude that $x\notin\pi(A)$. Similarly to the above discussion, we have $y\notin\pi(A)$. On the other hand, we know that $p+\varepsilon\in\mu(PGL(2,p))$ and so every two prime divisors of $p+\varepsilon$ are joined to each other. Therefore by the above discussion we conclude that $y\in\pi(N)$ or $x\in\pi(N)$. Since N is nilpotent, $x\sim r$ or $y\sim r$ in $\Gamma(G)$, for every $2\neq r\in\pi(p-\varepsilon)$. So we get a contradiction by Figure 1.

(b.2) Let $p_0=2$. We note that $(q^2-1)/(p',q-1)$ divides the order of maximal toruses in the form of $((q^i-1)(q^j-1))/((p',q-1)(q-1))$, where $i+j=p'$. Since $p'\geq 5$, by Lemma 2.15, there exists $2\neq s\in\pi((q^2-1)/(p',q-1))$. So we have $s\sim q^i-1$ in $\Gamma(G)$, for every $1\leq i\leq p'-1$. Therefore $\pi_1(P)\subseteq\pi(p-1)$ or $\pi_1(P)\subseteq\pi(p+1)$ and similarly to (b.1) we get a contradiction.

If $P\cong A_{p'}(q)$, where $(q-1)\mid(p'+1)$, ${}^2A_{p'-1}(q)$ or ${}^2A_{p'}(q)$, where $(q+1)\mid(p'+1)$ and $(p',q)\neq(3,3),(5,2)$, then we get a contradiction similarly.

Case 3. Let $P\cong A_1(q)$, where $4|(q+1)$ and $q=p_0^{\beta}$. Then $\pi_2(P)=\pi(q)$ and $\pi_3(P)=\pi((q-1)/2)$. So we have the following subcases.

(a) Let $\pi_2(P) = \{p\}$. Then $p = p_0$ and $\pi((q+1)(q-1)) \subseteq \pi(p^2-1)$. Therefore $\pi(p^{2\beta}-1) \subseteq \pi(p^2-1)$, which implies that $\beta = 1$ and $P \cong A_1(p)$, by Lemma 2.18. We claim that $\pi(N) \subseteq \pi(p-1)$. Let there exist $2 \neq s \in \pi(N) \cap \pi(p+1)$. Let U be the group of upper triangular matrices in $SL(2,p)$. Then U has a normal subgroup B of order p and the diagonal matrices are complements for B of order $p-1$. This gives a $p:(p-1)$ subgroup in $SL(2,p)$. Passing to the quotient modulo $\{I,-I\}$ gives the subgroup $p:(p-1)/2$ in $PSL(2,p)$. By Lemma 2.4, for every $2 \neq r \in \pi(p-1)$ we have $r \sim s$, which is a contradiction. Therefore $\pi(N) \subseteq \pi(p-1)$. If $2 \nmid |N|$ and $p \equiv 5$, 11 (mod 12), then by Lemma 2.8, we have $N = 1$. By Lemma 2.3, we have $A \leq Out(P)$, and so $A \leq \mathbf{Z}_2$.

(b) Let $\pi_3(P) = \{p\}$. So $(q-1)/2 = p^\alpha$, for some $\alpha > 0$, and $\pi(q(q+1)) \subseteq \pi(p^2-1)$. By Lemma 2.17, we have either $(p_0, \beta, p, \alpha) = (3, 5, 11, 2)$, which implies that $61 \in \pi(q+1) \subseteq \pi(p^2-1) = \pi(120)$, which is impossible; or $\alpha = \beta = 2$; or $\alpha = 1$; or $\beta = 1$. If $\alpha = \beta = 2$, then $p_0 \mid (2p^2+1)$. On the other hand, $p_0 \mid (p^2-1)$, which implies that $p_0 = 3$ and $p = 2$, which is a contradiction. If $\beta = 1$, then $p_0 = 2p^\alpha + 1$. On the other hand, we know that $p_0 \mid (p^2-1)$ and so $p_0 \mid (p^{2\alpha}-1)$. Therefore $p_0 \mid (4(p^{2\alpha}-1) - (4p^{2\alpha}-1))$ and so $p_0 = 3$. Thus $3 = 2p^\alpha + 1$, which is a contradiction. If $\alpha = 1$, then $p_0^\beta = 2p+1$ and so $p+1 = (p_0^\beta+1)/2$ and $p-1 = (p_0^\beta-3)/2$. We know that $p_0 \mid (p-1)$ or $p_0 \mid (p+1)$. If $p_0 \mid (p+1)$, then $p_0 = 1$, which is a contradiction. If $p_0 \mid (p-1)$, then $p_0 = 3$ and $p = (3^\beta-1)/2$, where β is an odd prime, by Remark 2.13. Therefore $P \cong A_1(3^\beta)$.

Let $\beta > 3$. We know that $p - 1 = 3(3^{\beta-1}-1)/2$. If $(3^{\beta-1}-1)/2 = 2^t$, for some integer t, then $3^{\beta-1} - 1 = 2^{t+1}$. By Lemma 2.15, we have $\beta = 3$, which is a contradiction. Therefore $(3^{\beta-1}-1)/2$ has an odd prime divisor. We claim that $\pi((3^{\beta-1}-1)/2) \nsubseteq \pi(A)$. Let $\pi((3^{\beta-1}-1)/2) \subseteq \pi(A)$. We know that $A \leq Out(P)$ and so $\pi(A) \subseteq \{2,\beta\}$. Therefore $3^{\beta-1} - 1 = 2^t\beta^s$, for some integers t, s. Since $\beta - 1$ is even, it follows that $(3^{(\beta-1)/2}-1)(3^{(\beta-1)/2}+1) = 2^t\beta^s$. Since $(3^{(\beta-1)/2}-1, 3^{(\beta-1)/2}+1) = 2$, by Lemma 2.15, we have $\beta = 5$, which implies that $p = 121$, and this is a contradiction. Thus there exists $2 \neq r \in \pi((3^{\beta-1}-1)/2) \setminus \pi(A)$. We note that $r \neq 3$ and $r \neq p = (3^\beta-1)/2$. If $r \mid (3^\beta+1)/2$, then $r = 2$, which is a contradiction and so $r \notin \pi(P)$. Therefore $r \in \pi(N)$. Since $r \notin \pi(P)$, by [**10**, Theorem

15.13], the Brauer character table in characteristic r and the ordinary character table of P are the same.

By Lemma 2.15, $(3^\beta+1)/2 = p+1$ has an odd prime divisor, say p_1. So $p_1 \le (3^\beta+1)/4$. Let $x \in P$, such that $o(x) = p_1$. Let $X = \langle x \rangle$.

By the notations of Lemma 2.12, let $m = (3^\beta + 1)/(2p_1)$ and $x = b^m\langle z\rangle$. Therefore $1 \le m \le (3^\beta - 3)/4$. Since $o(b)$ is even and $o(x)$ is odd, it follows that m is even. By Lemma 2.12, we will show that for every ordinary character ϕ of P, $\langle \phi|_X, 1|_X\rangle > 0$. Since β is an odd prime, it follows that $3^\beta \equiv -1 \pmod 4$. By using the tables in Lemma 2.12, we have

$$\begin{aligned}
\langle 1|_X, 1|_X\rangle &= 1 > 0;\\
\langle \psi|_X, 1|_X\rangle &= \frac{1}{p_1}(3^\beta + (p_1-1)(-1))\\
&\ge \frac{1}{p_1}(3^\beta - (3^\beta-3)/4) > 0;\\
\langle \chi_i|_X, 1|_X\rangle &= \frac{1}{p_1}(3^\beta+1) > 0, \text{ for } i = 2,4,6,\dots,(3^\beta-3)/2;\\
\langle \eta_1|_X, 1|_X\rangle &= \frac{1}{p_1}((3^\beta-1)/2 + (p_1-1)(-1)^{m+1})\\
&\ge \frac{1}{p_1}((3^\beta-1)/2 - (3^\beta-3)/4) > 0;\\
\langle \eta_2|_X, 1|_X\rangle &= \langle \eta_1|_X, 1|_X\rangle > 0;\\
\langle \theta_j|_X, 1|_X\rangle &= \frac{1}{p_1}\left(3^\beta - 1 + \sum_{t=1}^{p_1-1}(-\sigma^{jmt} - \sigma^{-jmt})\right)\\
&= \frac{1}{p_1}(3^\beta+1) > 0,\\
&\qquad \text{for } j = 2,4,6,\dots,(3^\beta-3)/2,\ (j,p_1) = 1;\\
\langle \theta_j|_X, 1|_X\rangle &= \frac{1}{p_1}\left(3^\beta - 1 + \sum_{t=1}^{p_1-1}(-\sigma^{jmt} - \sigma^{-jmt})\right)\\
&= \frac{1}{p_1}(3^\beta - 1 - 2(p_1-1))\\
&\ge \frac{1}{p_1}(3^\beta - 1 - (3^\beta-3)/2) > 0,\\
&\qquad \text{for } j = 2,4,6,\dots,(3^\beta-3)/2,\ (j,p_1) \ne 1.
\end{aligned}$$

We note that in the above computations $\sum_{t=1}^{p_1-1} \sigma^{jmt} = -1$, where $(j, p_1) = 1$, since σ^{jm} is the p_1th root of unity.

By Lemma 2.11, it follows that $r \sim p_1$, which is a contradiction by Figure 1.

We know that every composition factor of a solvable group is abelian. We see that N is nilpotent and $A \leq \mathbf{Z}_2$. Therefore N and A do not have any nonabelian composition factor. Therefore $P \cong A_1(p) \cong PSL(2,p)$ is the only nonabelian composition factor of G.

If $\beta = 3$, then $p = 13$. So $P \cong PSL(2,27)$ and by Lemma 2.3, $A \leq Out(PSL(2,27))$ and $\pi(N) \subseteq \{2,3,7\}$. If $2 \in \pi(N)$, and x is an element of order 13 in P, then by [**11**], $\langle \phi|_{\langle x \rangle}, 1|_{\langle x \rangle} \rangle > 0$, for every Brauer character ϕ of P of characteristic 2. Now Lemma 2.11 implies that $2 \sim 13$, which is a contradiction. If $7 \in \pi(N)$, then similarly we get a contradiction. Therefore N is a 3-group. By using [**5**], we know that $\Gamma(PSL(2,27).3) = \Gamma(PGL(2,13))$.

If $P \cong PSL(2,13)$, then similarly to the above discussion, N is a 2-group.

Similar to Case 3, if $P \cong A_1(q)$, where $4 \mid (q-1)$, then we conclude that $P \cong A_1(p)$.

Let $P \cong A_1(q)$, where $q = 2^\beta$, for some $\beta > 0$.

(a) Let $\pi_2(P) = \pi(q-1) = \{p\}$. Thus $q - 1 = p^\alpha$, for some $\alpha > 0$. Therefore $\alpha = 1$. It follows that p is a Mersenne prime, which is excluded.

(b) Let $\pi_3(P) = \pi(q+1) = \{p\}$. Thus $q + 1 = p^\alpha$, for some $\alpha > 0$. Therefore either $(p, \alpha, \beta) = (3, 2, 3)$; or $\alpha = 1$. It follows that p is a Fermat prime, which is excluded.

Case 4. Let $P \cong B_n(q)$, where $n = 2^m \geq 4$ and $q = p_0^\beta$ is odd. Therefore

$$\pi_1(P) = \pi(q(q^n - 1)\prod_{i=1}^{n-1}(q^{2i} - 1)) \subseteq \pi(p^2 - 1), \tag{3}$$
$$(q^n + 1)/2 = p^\alpha, \text{ for some } \alpha > 0.$$

So $q^n + 1 = 2p^\alpha$, which implies that $\alpha = 1$, by Lemma 2.17 and our assumptions. Thus $(q^n + 1)/2 = p$, $(q^n - 1)/2 = p - 1$ and $(q^n + 3)/2 = p + 1$. By (3), we know that either $p_0 \mid (p - 1)$, which implies that $p_0 \mid (q^n - 1)$, and so $p_0 = 1$; or $p_0 \mid (p + 1)$, which implies that $p_0 \mid (q^n + 3)$, and so $p_0 = 3$. Therefore $q = 3^\beta$. On the other hand, by Lemma 2.18, $3^{2\beta(n-1)} - 1$ has a primitive prime, say x. Then by (3), $x \mid (p + 1)$ or $x \mid (p - 1)$. If $x \mid (p + 1)$, then $x \mid (q^n + 3)$, which implies that $x \mid (3^{\beta n-1} + 1)$. On the other hand, $x \mid (3^{\beta(n-1)} + 1)$ and so $x \mid (3^{\beta-1} - 1)$. Therefore $2\beta(n - 1) \leq \beta - 1$, which implies that $2\beta < \beta - 1$, and this is a contradiction. If $x \mid (p - 1)$, then $x \mid (q^n - 1)$, which implies that $2(n - 1)\beta \leq n\beta$, and this is a contradiction by our assumptions.

If $P \cong B_{p'}(3)$, $C_n(q)$, where $n = 2^m \geq 2$, $C_{p'}(q)$, where $q = 2, 3$, $D_{p'}(q)$, where $p' \geq 5$ and $q = 2, 3, 5$ or $D_{p'+1}(q)$, where $q = 2, 3$, then we get a contradiction similarly.

Case 5. Let $P \cong {}^2D_n(q)$, where $n = 2^m \geq 4$ and $q = p_0^\beta$. Therefore

$$(4)\qquad \begin{gathered} \pi_1(P) = \pi\left(q \prod_{i=1}^{n-1} (q^{2i} - 1)\right) \subseteq \pi(p^2 - 1), \\ \frac{q^n + 1}{(2, q + 1)} = p^\alpha, \text{ for some } \alpha > 0. \end{gathered}$$

Let q be odd. Then $q^n + 1 = 2p^\alpha$, and so, by Lemma 2.17, we have $\alpha = 1$ and hence $(q^n + 1)/2 = p$. Thus $(q^n + 3)/2 = p + 1$ and $(q^n - 1)/2 = p - 1$. We know that $p_0 \mid (p^2 - 1)$ and we can easily see that $p_0 \nmid (p - 1)$. Therefore $p_0 \mid (p + 1)$ and so $p_0 = 3$, which implies that $q = 3^\beta$. By Lemma 2.18, $3^{2\beta(n-1)} - 1$ has a primitive prime, say x. By (4), we have $x \mid (p+1)$ or $x \mid (p-1)$. If $x \mid (p+1)$, then $x \mid (3^{\beta n} + 3)$ and so $x \mid (3^{\beta n-1} + 1)$. On the other hand, $x \mid (3^{\beta(n-1)} + 1)$, since x is a primitive prime of $3^{2\beta(n-1)} - 1$, and so $x \mid (3^{\beta-1} - 1)$. Therefore $2\beta(n-1) \leq \beta - 1$, which is a contradiction. If $x \mid (p-1)$, then $x \mid (q^n - 1)$, which implies that $2(n - 1)\beta \leq n\beta$, and this is a contradiction, by our assumptions. Therefore q is even. Then $p^\alpha = q^n + 1$ and by Lemma 2.15, $\alpha = 1$ and p is a Fermat prime, which is excluded.

If $P \cong {}^2D_n(2)$, where $n = 2^m + 1 \geq 5$, ${}^2D_n(3)$, where $n = 2^m + 1 \neq p'$ and $m \geq 2$ or ${}^2D_{p'}(3)$, where $p' \geq 5$, then we get a contradiction similarly.

Case 6. Let $P \cong G_2(q)$, where $q = p_0^\beta$.

We must consider 3 subcases. Let $q \equiv -1 \pmod 3$ and $q > 2$. Then we have

$$\pi_1(P) = \pi(q(q^3+1)(q^2-1)) \subseteq \pi(p^2-1),$$
$$q^2+q+1 = p^\alpha, \text{ for some } \alpha > 0. \tag{5}$$

We claim that q is a Fermat prime. Let $x \in \pi(q-1)$. By (5), $x \mid (p^2-1)$. If $x \mid (p-1)$, then $x \mid (p^\alpha - 1)$. Thus $x \mid (q^2+q)$, since $q^2+q = p^\alpha - 1$, and hence $x \mid (q+1)$, which implies that $x = 2$. Let $x \mid (p+1)$. If α is even, then $x \mid (p^\alpha - 1)$, and similarly to the above case $x = 2$. If α is odd, then $x \mid (p^\alpha + 1)$. Therefore $x \mid (q^2+q+2)$, which implies that $x \mid (q+3)$ and so $x = 2$. Thus q is a Fermat prime and hence $q = 2^k + 1$, for some integer k.

By [**31**], $q^2 - q + 1$ is the order of a maximal torus of P. Therefore by (5), $\pi(q^2-q+1) \subseteq \pi(p-1)$ or $\pi(q^2-q+1) \subseteq \pi(p+1)$. Let $\pi(q^2-q+1) \subseteq \pi(p-1)$. If $x \in \pi(q^2-q+1)$, then $x \mid (p-1)$ and so $x \mid (p^\alpha - 1)$. Therefore $x \mid q(q+1)$, which implies that $x \mid (2q-1)$. On the other hand, $x \mid (q+1)$ and hence $x = 3$. It follows that $q^2 - q + 1 = 3^t$, for some integer t. Thus $(2^k+1)^2 - (2^k+1) + 1 = 3^t$ and so $2^{2k} + 2^k = 3^t - 1$. If t is odd, then $|3^t - 1|_2 = 2$ and hence $k = 1$, which is a contradiction since $3^t - 1 = 6$. Therefore t is even and so by Lemma 2.16, we have $t = 2^{k-2}l$, where l is an odd number. Therefore $2^k(2^k+1) = 3^{2^{k-2}l} - 1$. For $k \geq 5$, we have $2^k(2^k+1) < 3^{2^{k-2}l} - 1$ and for $k \leq 4$, the equation has no solution. Therefore $\pi(q^2-q+1) \subseteq \pi(p+1)$. If $x \in \pi(q^2-q+1)$, then $x \mid (p+1)$. If α is even, then $x \mid (p^\alpha - 1)$ and we get a contradiction similarly. If α is odd, then it follows that $x \mid (p^\alpha + 1)$ and hence $x \mid (q^2+q+2)$. Therefore $x \mid (2q+1)$, which implies that $x \mid (3q-2)$. So $x = 7$, and hence $q^2 - q + 1 = 7^t$, for some integer t. Thus $(2^k+1)^2 - (2^k+1) + 1 = 7^t$. Therefore $2^{2k} + 2^k = 7^t - 1$, and we get a contradiction similarly to the above discussion.

If $q \equiv 0, 1 \pmod 3$, then similarly we get a contradiction.

Case 7. Let $P \cong E_6(q)$. Therefore

$$\pi_1(P) = \pi(q(q^5-1)(q^8-1)(q^{12}-1)) \subseteq \pi(p^2-1),$$
$$\frac{q^6+q^3+1}{(3, q-1)} = p^\alpha, \text{ for some } \alpha > 0. \tag{6}$$

We have the following subcases.

(a) Let $(3, q-1) = 3$. Then $(q^6+q^3+1)/3 = p^\alpha$. Let $x \in \pi(q^3+1)$. By (6), $x \mid (p^2-1)$. If $x \mid (p-1)$, then $x \mid (p^\alpha - 1)$, which implies that $x \mid (q^6+q^3-2)$ and so $x=2$. Let $x \mid (p+1)$. If α is even, then $x \mid (p^\alpha-1)$, and similarly $x=2$. If α is odd, then $x \mid (p^\alpha+1)$ and hence $x \mid (q^6+q^3+4)$, which implies that $x=2$. Therefore $q^3+1=2^t$, for some integer t, and this is a contradiction, by Lemma 2.15.

(b) Let $(3,q-1)=1$. Then $q^6+q^3+1=p^\alpha$. Let $x \in \pi(q^3-1)$. By (6), $x \mid (p^2-1)$. If $x \mid (p-1)$, then $x \mid (p^\alpha-1)$, which implies that $x \mid (q^3+1)$, and hence $x=2$. If $x \mid (p+1)$, then similarly we conclude that $x=2$. It follows that $q^3-1=2^t$, for some integer t, and this is a contradiction, by Lemma 2.15.

If $P \cong {}^3D_4(q)$, $F_4(q)$, ${}^2E_6(q)$ or ${}^2G_2(q)$, where $q=3^{2n+1}$, then we get a contradiction similarly and we omit the proof of these cases for convenience.

Case 8. Let $P \cong {}^2B_2(q)$, where $q=2^{2n+1}>2$. We have the following subcases.

(a) Let $\pi_2(P)=\pi(q-1)=\{p\}$. So $q-1=p^\alpha$, for some $\alpha>0$. By Lemma 2.15, we have $\alpha=1$, and p is a Mersenne prime, which is a contradiction.

(b) Let $\pi_3(P)=\pi(q-\sqrt{2q}+1)=\{p\}$. So we have $2^{2n+1}-2^{n+1}+1=p^\alpha$, for some $\alpha>0$. Let x be a primitive prime of $q-1=2^{2n+1}-1$. If $x \mid (p-1)$, then $x \mid (p^\alpha-1)$. It follows that $x \mid (2^n-1)$, which is a contradiction. Therefore $x \mid (p+1)$. If α is even, then $x \mid (p^\alpha-1)$ and similarly we get a contradiction. If α is odd, then $x \mid (p^\alpha+1)$ and therefore $x \mid (2^{2n+1}-2^{n+1}+2)$. It follows that $x \mid (2^{n+1}-3)$ and hence $x \mid (2^n(2^{n+1}-3)-(2^{2n+1}-1))$. So $x \mid (3\times 2^n-1)$, which implies that $x=7$. Since $\mathrm{ord}_7 2=3$, we have $n=1$ and $p=5$, which is excluded.

(c) Let $\pi_4(P)=\pi(q+\sqrt{2q}+1)=\{p\}$. So we have $2^{2n+1}+2^{n+1}+1=p^\alpha$, for some $\alpha>0$. Let x be a primitive prime of $q-1=2^{2n+1}-1$. If $x \mid (p-1)$, then $x \mid (p^\alpha-1)$. It follows that $x \mid (2^n+1)$, which is a contradiction. Therefore $x \mid (p+1)$. If α is even, then similarly we get a contradiction. If α is odd, then $x \mid (p^\alpha+1)$ and therefore $x \mid (2^{2n+1}+2^{n+1}+2)$. It follows that $x \mid (2^{n+1}+3)$ and hence $x \mid (2^n(2^{n+1}+3)-(2^{2n+1}-1))$. So $x \mid (3\times 2^n+1)$, which implies that $x=7$. Since $\mathrm{ord}_7 2=3$, we have $n=1$ and $p=13$. Therefore $q-\sqrt{2q}+1=5$, but $5 \notin \pi(13^2-1)$, which is a contradiction.

Case 9. Let $P \cong {}^2F_4(q)$, where $q=2^{2n+1}>2$. Therefore

$$\pi_1(P)=\pi(q(q^4-1)(q^3+1)) \subseteq \pi(p^2-1). \tag{7}$$

We have the following subcases.

(a) Let $\pi(q^2-\sqrt{2q^3}+q-\sqrt{2q}+1)=\{p\}$. So $2^{2(2n+1)}-2^{3n+2}+2^{2n+1}-2^{n+1}+1=p^\alpha$, for some $\alpha>0$. Therefore $2^{n+1}(2^n-1)(2^{2n+1}+1)=p^\alpha-1$. Let x be a primitive prime of $2^{6(2n+1)}-1$. So $x\mid(q^3+1)$ and hence by (7), $x\mid(p+1)$ or $x\mid(p-1)$. If $x\mid(p-1)$, then $x\mid(p^\alpha-1)$. Therefore $x\mid(2^n-1)$ or $x\mid(2^{2n+1}+1)$, which is a contradiction, since x is a primitive prime of $2^{6(2n+1)}-1$. If $x\mid(p+1)$ and α is even, then $x\mid(p^\alpha-1)$ and we get a contradiction similarly. If α is odd, then $x\mid(p^\alpha+1)$ and so $x\mid(2^{2(2n+1)}-2^{3n+2}+2^{2n+1}-2^{n+1}+2)$. Since x is a primitive prime of $2^{6(2n+1)}-1$, hence $x\mid(2^{2(2n+1)}-2^{2n+1}+1)$. It follows that $x\mid(2^{3n+2}-2^{2n+2}+2^{n+1}-1)$. Therefore x is a divisor of $(2^{2(2n+1)}-2^{2n+1}+1)-2^n(2^{3n+2}-2^{2n+2}+2^{n+1}-1)=2^{3n+2}-2^{2n+2}+2^n+1$. So $x\mid(2^{n-1}-1)$, which is a contradiction, since x is a primitive prime of $2^{6(2n+1)}-1$.

(b) If $\pi(q^2+\sqrt{2q^3}+q+\sqrt{2q}+1)=\{p\}$, then similarly we get a contradiction.

Case 10. Let $P\cong E_8(q)$ and $q\equiv 0,1,4 \pmod 5$. Therefore

(8) $\pi_1(P)=\pi(q(q^8-1)(q^{10}-1)(q^{12}-1)(q^{14}-1)(q^{18}-1))\subseteq\pi(p^2-1)$.

We have the following subcases.

(a) Let $\pi_2(P)=\pi((q^{10}+1)/(q^2+1))=\{p\}$. Therefore $(q^{10}+1)/(q^2+1)=p^\alpha$, for some $\alpha>0$. We know that $(q^{24}-1)\mid |P|$. Let x be a primitive prime of $q^{24}-1$. So $x\mid(q^8-q^4+1)$, and so we have $x\in\pi(p-1)$ or $x\in\pi(p+1)$. If $x\in\pi(p-1)$, then $x\mid(p^\alpha-1)$ and hence $x\mid(q^8-1)$, which is a contradiction. If $x\in\pi(p+1)$ and α is even, then similarly we get a contradiction. If α is odd, then $x\mid(p^\alpha+1)$, which implies that $x\mid(q^{10}+q^2+2)$ and it follows that $x\mid(q^6+2)$. Therefore $x\mid(q^4+2q^2-1)$ and consequently x is a divisor of $(q^4(q^4+2q^2-1)-(q^8-q^4+1))=(2q^6-1)$, which implies that $x=5$. This shows that for $q\equiv 0 \pmod 5$, we get a contradiction. Therefore $5\nmid q$ and so $5\mid(q^4-1)$, which is a contradiction, since x is a primitive prime of $q^{24}-1$.

(b) Let $\pi_3(P)=\pi(q^8-q^4+1)=\{p\}$. Then $q^8-q^4+1=p^\alpha$, for some $\alpha>0$. Let x be a primitive prime of $q^{20}-1$. Obviously $x\in\pi_2(P)$ and so $x\neq p$. If $x\in\pi(p-1)$, then $x\mid(p^\alpha-1)$, which implies that $x\mid(q^4-1)$, and this is a contradiction. If $x\in\pi(p+1)$ and α is even, then we get a contradiction similarly. If α is odd, then $x\mid(p^\alpha+1)$, which implies that $x \mid (q^8 - q^4 + 2)$. Since x is a primitive prime of $q^{20} - 1$, then $x \mid (q^{10} + 1)$ and therefore $x \mid (q^6 - 2q^2 + 1)$. It follows that $x \mid (q^4 - q^2 + 2)$ and hence $x \mid (q^4 - 4q^2 + 1)$. Thus $x \mid (3q^2 + 1)$, which implies that $x \mid (q^8 - 3)$, since $x \mid (q^{10} + 1)$. Therefore $x \mid (q^4 - 5)$ and so $x \mid (q^8 - 25)$, which implies that $x \mid 22$. Therefore $x = 11$. Also $\mathrm{ord}_{11} q = 20$, since 11 is a primitive prime of $q^{20} - 1$. Thus $20 \mid (11 - 1)$, which is a contradiction.

(c) Let $\pi_4(P) = \pi(q^8 - q^7 + q^5 - q^4 + q^3 - q + 1) = \{p\}$. Therefore $q^8 - q^7 + q^5 - q^4 + q^3 - q + 1 = p^\alpha$, for some $\alpha > 0$, and hence $q(q^2 - 1)(q^5 - q^4 + q^3 + 1) = p^\alpha - 1$. Let x be a primitive prime of $q^{10} - 1$. Then $x \mid (q^5 + 1)$, and we have $x \in \pi(p - 1)$ or $x \in \pi(p + 1)$. If $x \mid (p - 1)$, then $x \mid (p^\alpha - 1)$, and hence $x \mid (q^5 - q^4 + q^3 + 1)$, since x is a primitive prime of $q^{10} - 1$. Therefore $x \mid (q - 1)$, which is a contradiction. If $x \in \pi(p+1)$ and α is even, then we get a contradiction similarly. Therefore α is odd. By [**31**], $(q^5 + 1)(q^2 - q + 1)(q \pm 1)$ are the orders of maximal toruses of P. Since $x \in \pi(p+1)$ and $x \mid (q^5 + 1)$, we have $\pi((q^5 + 1)(q^2 - q + 1)(q \pm 1)) \subseteq \pi(p + 1)$. If $y \in \pi(q^2 - 1)$, then $y \mid (p + 1)$, which implies that $y \mid (p^\alpha + 1)$. On the other hand, $y \mid (p^\alpha - 1)$, since $q(q^2 - 1)(q^5 - q^4 + q^3 + 1) = p^\alpha - 1$. It follows that $y = 2$. Hence $q^2 - 1 = 2^t$, for some integer t, which implies that $q = 3$ and this is a contradiction, since $q \equiv 0, 1, 4 \pmod 5$.

(d) Let $\pi_5(P) = \pi(q^8 + q^7 - q^5 - q^4 - q^3 + q + 1) = \{p\}$. We suppose that x is a primitive prime of $q^5 - 1$, and we get a contradiction similarly to (c).

If $P \cong E_8(q)$ and $q \equiv 2, 3 \pmod 5$, then by small modification of the above proof we get a contradiction.

Case 11. If P is a sporadic simple group or P is isomorphic to ${}^2A_3(2)$, ${}^2F_4(2)'$, $A_2(4)$, ${}^2A_5(2)$, $E_7(2)$, $E_7(3)$ or ${}^2E_6(2)$, then easily we get a contradiction. For example if $P \cong M$, then $p = 71$, by Remark 2.1. Therefore $59 \in \pi(p^2 - 1)$, which is a contradiction.

So if $p \neq 13$, then $PGL(2,p)$ is NCF-distinguishable. If $p = 13$, then the only non-abelian composition factor of G is $PSL(2,13)$ or $PSL(2,27)$. Now the proof of the main theorem is completed. ◻

Remark 3.2. By Lemmas 2.5 and 2.7, $h(PGL(2,p)) = \infty$. So N is not always trivial.

Corollary 3.3. *Let G be a group and p a prime number such that $\pi_e(G) = \pi_e(PGL(2,p))$ and $|G| = |PGL(2,p)|$, where p is not a Mersenne or Fermat prime and $p \neq 11$, 19. Then $G \cong PGL(2,p)$.*

Proof. Since $\pi_e(G) = \pi_e(PGL(2,p))$, then we conclude that $\Gamma(G) = \Gamma(PGL(2,p))$. Therefore $Z(G) = 1$. So by the main theorem, G has a normal series $1 \trianglelefteq N \trianglelefteq N.P \trianglelefteq N.P.A = G$, such that N is a nilpotent group. If $p \neq 13$, then $P \cong PSL(2,p)$ and $A \leq Out(PSL(2,p)) \cong \mathbf{Z}_2$. Since $|G| = |PGL(2,p)|$, we have $|N| \mid 2$. If $|N| = 2$, then $N \leq Z(G)$, which is a contradiction, since $Z(G) = 1$. Thus $|N| = 1$ and $|A| = 2$. So the generator of A is a diagonal automorphism and we conclude that $G \cong PGL(2,p)$. If $p = 13$, then $P \cong PSL(2,13)$ or $P \cong PSL(2,27)$ and $A \leq Out(P)$. Since $|PSL(2,27)| > |PGL(2,13)|$, it follows that $P \cong PSL(2,13)$ and similarly to above discussion $G \cong PGL(2,13)$. $\square$

Remark 3.4. We note that as a consequence of our main theorem, we give a new proof for Step 1 and Step 2 of the main result in [**26**], where $p \neq 11$, 13, 19 and p is not a Mersenne or Fermat prime.

Acknowledgments. The authors express their gratitude to the referee for valuable suggestions.

REFERENCES

1. Z. Akhlaghi, M. Khatami and B. Khosravi, *Quasirecognition by prime graph of the simple group* $^2F_4(q)$, Acta. Math. Hungar. **122** (2009), 387–397.

2. V.P. Burichenko, *Extensions of abelian 2-groups by* $L_2(q)$ *with an irreducible action*, Algebra Logic **39** (2000), 160–183.

3. R. Burkhardt, *Die zerlegungsmatrizen der gruppen* $PSL(2,p^f)$, J. Algebra **40** (1976), 75–96.

4. G.Y. Chen, V.D. Mazurov, W.J. Shi, A.V. Vasil'ev and A.Kh. Zhurtov, *Recognition of the finite almost simple groups* $PGL_2(q)$ *by their spectrum*, J. Group Theory **10** (2007), 71–85.

5. J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of finite groups*, Oxford University Press, Oxford, 1985.

6. P. Crescenzo, *A diophantine equation which arises in the theory of finite groups*, Adv. Math. **17** (1975), 25–29.

7. K.E. Gehles, *Ordinary characters of finite special linear groups*, M.Sc. dissertation, August 2002, School of Mathematics and Statistics, University of St. Andrews.

8. M. Hagie, *The prime graph of a sporadic simple group*, Comm. Algebra **31** (2003), 4405–4424.

9. N. Iiyori and H. Yamaki, *Prime graph components of the simple groups of Lie type over the field of even characteristic*, J. Algebra **155** (1993), 335–343.

10. I.M. Issacs, *Character theory of finite groups*, Academic Press, New York, 1976.

11. C. Jansen, K. Lux, R. Parker and R. Wilson, *An atlas of Brauer characters*, Clarendon Press, Oxford, 1995.

12. A. Khosravi and B. Khosravi, *Quasirecognition by prime graph of the simple group* ${}^2G_2(q)$, Siberian Math. J. **48** (2007), 570–577.

13. B. Khosravi, *n-recognition by prime graph of the simple group $PSL(2,q)$*, J. Algebra Appl. **7** (2008), 735–748.

14. B. Khosravi and S. Salehi Amiri, *On the prime graph of $L_2(q)$ where $q = p^\alpha < 100$*, Quasigroups Related Systems **14** (2006), 179–190.

15. B. Khosravi, B. Khosravi and B. Khosravi, *Groups with the same prime graph as a* CIT *simple group*, Houston J. Math. **33** (2007), 967–977.

16. ———, *On the prime graph of $PSL(2,p)$ where $p > 3$ is a prime number*, Acta. Math. Hungar. **116** (2007), 295–307.

17. ———, *Characterizability of $PSL(p+1,q)$ by its order components*, Houston J. Math. **32** (2006), 683–700.

18. ———, *A characterization of the simple group $L_{16}(2)$ by its prime graph*, Manuscr. Math. **126** (2008), 49–58.

19. ———, *2-recognizability of $PSL(2,p^2)$ by the prime graph*, Siberian Math. J. **49** (2008), 749–757.

20. A.S. Kondrat'ev, *Prime graph components of finite simple group*, Math. USSR-SB. **67** (1990), 235–247.

21. M.S. Lucido, *The diameter of the prime graph of a finite group*, J. Group Theory **2** (1999), 157–172.

22. V.D. Mazurov, *Characterizations of groups by arithmetic properties*, Algebra Colloquium **11** (2004), 129–140.

23. ———, *Characterizations of finite groups by sets of their element orders*, Algebra Logic **36** (1997), 23–32.

24. ———, *Recognition of finite simple groups $S_4(q)$ by their element orders*, Algebra Logic **41** (2002), 93–110.

25. V.D. Mazurov, M.C. Xu and H.P. Cao, *Recognition of finite simple groups $L_3(2^m)$ and $U_3(2^m)$ by their element orders*, Algebra Logic **39** (2000), 324–334.

26. A.R. Moghadamfar and W.J. Shi, *The characterization of almost simple groups $PGL(2,p)$ by their element orders*, Comm. Algebra **32** (2004), 3327–3338.

27. C.E. Praeger and W. Shi, *A characterization of some alternating and symmetric groups*, Comm. Algebra **22** (1994), 1507–1530.

28. W. Sierpiński, *Elementary theory of numbers*, Mono. matem. **42**, Panstwowe Wydawnictwo Naukowe, Warsaw, 1964 (translated from Polish by A. Hulanicki).

29. W.B. Stewart, *Groups having strongly self-centralizing* 3*-centralizers*, Proc. London Math. Soc. **26** (1973), 653–680.

30. The GAP Group, GAP–*Groups, algorithms and programming*, Vers. 4.4.7 (2006); http://www.gap-system.org.

31. A.V. Vasil'ev and E.P. Vdovin, *An adjacency criterion for the prime graph of a finite simple group*, Algebra Logic **44** (2005), 381–406.

32. J.S. Williams, *Prime graph components of finite groups*, J. Algebra **69** (1981), 487–513.

33. A.V. Zavarnitsin, *Recognition of finite groups by the prime graph*, Algebra Logic **43** (2006), 220–231.

34. K. Zsigmondy, *Zur theorie der potenzreste*, Monatsh. Math. Phys. **3** (1892), 265–284.

Dept. of Pure Math., Amirkabir University of Technology (Tehran Polytechnic), 424, Hafez Ave., Tehran 15914, Iran
Email address: maryam_khatami81@yahoo.com

Dept. of Pure Math., Faculty of Math. and Computer Sci., Amirkabir University of Technology (Tehran Polytechnic), 424, Hafez Ave., Tehran 15914, Iran
Email address: khosravibbb@yahoo.com

Dept. of Pure Math., Amirkabir University of Technology (Tehran Polytechnic), 424, Hafez Ave., Tehran 15914, Iran
Email address: zeinab_akhlaghi@yahoo.com