*Glasgow Math. J.* **54** (2012) 345–354. © Glasgow Mathematical Journal Trust 2011.
doi:10.1017/S0017089511000644.

# FACTORIZATION NUMBERS OF SOME FINITE GROUPS

F. SAEEDI

*Department of Mathematics, Mashhad Branch, Islamic Azad University, Mashhad, Iran.*
*e-mail: saeedi@mshdiau.ac.ir*

and M. FARROKHI D. G.

*Department of Pure Mathematics, Ferdowsi University of Mashhad, Mashhad, Iran.*
*e-mail: m.farrokhi.d.g@gmail.com*

(Received 16 August 2011; accepted 24 September 2011; first published online 12 December 2011)

**Abstract.** For a finite group $G$, let $F_2(G)$ be the number of factorizations $G = AB$ of the group $G$, where $A$ and $B$ are subgroups of $G$. We compute $F_2(G)$ for certain classes of groups, including cyclic groups $\mathbb{Z}_n$, elementary abelian $p$-groups $\mathbb{Z}_p^n$, dihedral groups $D_{2n}$, generalised quaternion groups $Q_{4n}$, quasi-dihedral 2-groups $QD_{2^n} (n \geq 4)$, modular $p$-groups $M_{p^n}$, projective general linear groups $PGL(2, p^n)$ and projective special linear groups $PSL(2, p^n)$.

2000 *Mathematics Subject Classification.* Primary 20D40, secondary 20P05.

**1. Introduction and Preliminaries.** Let $G$ be a group and $A$ and $B$ be subgroups of $G$. If $G = AB$, then $G$ is said to be *factorized* by $A$ and $B$ and the expression $G = AB$ is said to be a *factorization* of $G$. The factorization of groups have been studied by various authors investigating those properties of groups that inherit from the subgroups in the factorization. In particular, there have been special attentions to those groups who have well-known structures and their factorizations is determined completely, say

(1) projective special linear groups $PSL(2, q)$ [**5**],
(2) projective special linear groups $PSL(3, q)$ and projective special unitary groups $PSU(3, q)$ [**1**],
(3) the simple groups $G_2(q)$ [**6**],
(4) sporadic simple groups [**2**],
(5) simple groups of Lie type of Lie rank 1 and 2 [**3**].

Now, let $G$ be a finite group and $F_2(G)$, the *factorization number* of $G$, be the number of factorizations of $G$.

Tărnăuceanu [**7**] defined the subgroup commutativity degree $scd(G)$ of $G$ as the proportion of the number of ordered pairs $(A, B)$ of subgroups of $G$ such that $AB = BA$ by $|L(G)|^2$, where $L(G)$ is the lattice of all subgroups of $G$, and he computed $scd(G)$ for some classes of groups, including dihedral groups $D_{2n}$, generalised quaternion 2-group $Q_{2^n}$, quasi-dihedral 2-groups $QD_{2^n}$ $(n \geq 4)$ and modular $p$-groups $M_{p^n}$. The factorization numbers could be applied to compute the subgroup commutativity degree of a given group $G$ for

$$scd(G) = \frac{1}{|L(G)|^2} \sum_{H \leq G} F_2(H).$$

Hence, to compute the subgroup commutativity degree of a finite group it is enough to know the factorization number of its subgroups.

We intend to obtain the factorizations of some other classes of groups, and hence compute their factorization numbers. To compute the number of solutions $(A, B)$ to the equation $G = AB$ we need to know the subgroups of $G$, the simplest of which are abelian groups. Also, the subgroups of dihedral groups $D_{2n}$, generalised quaternion groups $Q_{4n}$, quasi-dihedral groups $QD_{2^n}(n \geq 4)$ and modular $p$-groups $M_{p^n}$ are known, and from a well-known theorem of Dickson (Hauptsatz II.8.27 in **[4]**) we know the isomorphism classes of subgroups of $PSL(2, p^n)$ and also $PGL(2, p^n)$. Our results give alternative formulas to Tărnăuceanu's results. Also, in a sequel to this paper, we will apply our results to compute the subgroup commutativity degree of projective special linear groups $PSL(2, q)$.

We begin with the following definition.

DEFINITION. If $f$ is a (strong) multiplicative arithmetic function, then

$$\Phi_f(n) = \sum_{\substack{a,\, b|n \\ \gcd(a,\, b) = 1}} f(ab).$$

It is straightforward to see that if $n = p_1^{a_1} \ldots p_m^{a_m}$, then

$$\Phi_f(n) = \prod_{i=1}^{m} \left(1 + 2\left(f(p_i) + \cdots + f\left(p_i^{a_i}\right)\right)\right).$$

In particular, if $f$ is strong multiplicative, then

$$\Phi_f(n) = \prod_{i=1}^{m} \left(2\frac{f(p_i)^{a_i+1} - 1}{f(p_i) - 1} - 1\right)$$

if $f(p_i) \neq 1$, for $i = 1, \ldots, k$ and

$$\Phi_1(n) = \prod_{i=1}^{m} (2a_i + 1).$$

Albeit the subgroups of finite abelian groups can be determined completely but the computation of the number of solutions $(A, B)$ to the equation $G = AB$ seems to be too complicated in general. Thus, we may take $G$ to be a finite abelian group of some special type.

Let $G = \langle x \rangle$ be a cyclic group of order $n$ and $A = \langle x^a \rangle$, $B = \langle x^b \rangle$ be subgroups of $G$, where $a, b$ are divisors of $n$. Then we can see that $G = AB$ if and only if $ai + bj \equiv 1 \pmod{n}$ for some integers $i, j$, which is equivalent to $\gcd(a, b, n) = \gcd(a, b) = 1$. Thus,

$$F_2(G) = \sum_{\substack{a,\, b|n \\ \gcd(a,\, b) = 1}} 1 = \Phi_1(n).$$

Utilising the above notations we have the following.

THEOREM 1.1. *If $G = \mathbb{Z}_n$ is a cyclic groups, then $F_2(G) = \Phi_1(n)$.*

https://doi.org/10.1017/S0017089511000644 Published online by Cambridge University Press

Another classes of finite abelian groups which can be handled simply are the elementary abelian $p$-groups as we consider below.

THEOREM 1.2. *If $G = \mathbb{Z}_p^n$ is an elementary abelian $p$-group, then*

$$F_2(G) = |L(G)|^2 - \sum_{i=0}^{n-1} \binom{n}{i}_p F_2(\mathbb{Z}_p^i),$$

*where $|L(G)| = \sum_{i=0}^{n} \binom{n}{i}_p$ is the number of subgroups of $G$ and*

$$\binom{n}{i}_p = \frac{(p^n - 1)\cdots(p-1)}{(p^i - 1)\cdots(p-1)(p^{n-i}-1)\cdots(p-1)}$$

*is the number of subgroups of $G$ of order $p^i$.*

*Proof.* Utilizing the notations in the theorem

$$|L(G)|^2 = \sum_{A,B \leq G} 1 = \sum_{i=0}^{n} \sum_{\substack{A,\,B \,\leq\, G \\ |AB| \,=\, p^i}} 1$$

$$= \sum_{i=0}^{n} \binom{n}{i}_p F_2(\mathbb{Z}_p^i) = \sum_{i=0}^{n-1} \binom{n}{i}_p F_2(\mathbb{Z}_p^i) + F_2(G),$$

which gives the desired result. □

**2. Dihedral, generalised quaternion, quasi-dihedral and modular $p$-groups.** To compute $F_2(G)$ for the classes of dihedral, generalised quaternion and quasi-dihedral groups we first need to set the following notation:

$$\delta_n = \sum_{1 \neq k | n} \frac{n}{k} \prod_{p_i \nmid \frac{n}{k}} (\alpha_i + 1) = \prod_{i=1}^{m} \left( \alpha_i + \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right) - n$$

for $n = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$. Since $D_{2n}$ can be expressed as a factor group of $Q_{4n}$ and $QD_{2^m}$ (if $n = 2^{m-2}$), it is enough to compute $F_2(D_{2n})$ in details and use it to compute $F_2(Q_{4n})$ and $QD(2^m)$. We begin with the case of dihedral groups.

THEOREM 2.1. *Let $G = D_{2n}$ $(n \geq 3)$ be a dihedral group. Then,*

$$F_2(G) = \begin{cases} \Phi_x(n) + 2\delta_n + 2n, & \text{odd } n, \\ \Phi_x(n) + 2\Phi_x\left(\frac{n}{2}\right) + 2\delta_n + 2n, & \text{even } n. \end{cases}$$

*where $\Phi_x(1) = 1$ and*

$$\Phi_x(n) = \prod_{i=1}^{m} \left( 2\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} - 1 \right)$$

*for $n = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$.*

*Proof.* Let $G = D_{2n} = \langle x, y : x^n = y^2 = 1, x^y = x^{-1} \rangle$ and $A, B \leq G$ such that $G = AB$ and let $n = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$. We divide the proof into three parts:

(1) $A$ and $B$ are cyclic.

If $A, B \leq \langle x\rangle$, then $AB \leq \langle x\rangle$, which is impossible. Without loss of generality assume that $B \nleq \langle x\rangle$. Then $|B| = 2$, $A \cap B = 1$ and $|G| = |A||B|$, which implies that $|A| = n$. Then $A = \langle x\rangle$ and so the number of solutions is $n$.

(2) One of the $A$ and $B$ is a dihedral group and the other is cyclic.

Without loss of generality we may assume that $A = \langle x^{\frac{n}{k}}, x^i y\rangle$, where $0 \leq i < \frac{n}{k}$ is a dihedral group of order $2k$ and $B = \langle x^j\rangle$ or $\langle x^j y\rangle$ is a cyclic group, where $0 \leq j < n$. First, suppose that $B = \langle x^j y\rangle$. If $A = G$, then we have $n$ different choices for $B$. Thus, we may assume that $A \neq G$. Clearly $|G| = |A||B|$ and we should have $n = 2k$ is even. Since an arbitrary element of $AB$ has the form $x^{2u}$, $x^{2u+i}y$, $x^{2u+j}y$ or $x^{2u+i-j}y$, one can easily see that $G = AB$ if and only if $i - j$ is odd. Thus, the number of solutions $(A, B)$ is $n + 2\binom{n}{2} = 2n$. Now suppose that $B = \langle x^j\rangle$, where $j$ divides $n$. Since an arbitrary element of $AB$ has the form $x^{\frac{n}{k}u+jv}$ or $x^{\frac{n}{k}u-jv+i}y$, one can easily see that $G = AB$ if and only if $\gcd\left(\frac{n}{k}, j\right) = 1$ and consequently there is $\delta_n = \sum_{1\neq k|n} \frac{n}{k} \prod_{p_t \nmid \frac{n}{k}} (\alpha_t + 1)$ solutions $(A, B)$, in which $\prod_{p_t \nmid \frac{n}{k}} (\alpha_t + 1)$ is the number of $j$s satisfying $\gcd\left(\frac{n}{k}, j\right) = 1$.

(3) $A$ and $B$ are dihedral groups.

Let $A = \langle x^{\frac{n}{k}}, x^i y\rangle$ and $B = \langle x^{\frac{n}{d}}, x^j y\rangle$ be dihedral groups of order $2k$ and $2d$, respectively, where $0 \leq i < \frac{n}{k}$ and $0 \leq j < \frac{n}{d}$. Let $l := \gcd\left(\frac{n}{k}, \frac{n}{d}\right)$. Then $\left\{\frac{n}{k}u + \frac{n}{d}v : u, v \in \mathbb{Z}\right\} = l\mathbb{Z}$. Since an arbitrary element of $AB$ has the form

$$x^{\frac{n}{k}u+\frac{n}{d}v},\ x^{\frac{n}{k}u+\frac{n}{d}v+j}y,\ x^{\frac{n}{k}u-\frac{n}{d}v+i}y \text{ or } x^{\frac{n}{k}u-\frac{n}{d}v+i-j},$$

either $l = 1$ and $G = AB$, or $l > 1$ and $\mathbb{Z} = l\mathbb{Z} \cup (l\mathbb{Z} + i - j)$, which is possible if and only if $l = 2$ and $i - j$ is odd. Thus, the number of solutions $(A, B)$ is

$$\sum_{\substack{1\neq k,\, d|n \\ \gcd(\frac{n}{k},\frac{n}{d})=1}} \frac{n}{k}\cdot\frac{n}{d} = \sum_{\substack{n\neq a,\, b|n \\ \gcd(a,b)=1}} ab = \Phi_x(n) - 2n$$

if $l = 1$ and

$$\sum_{\substack{1\neq k,\, d|n \\ \gcd(\frac{n}{k},\frac{n}{d})=2}} \frac{1}{2}\cdot\frac{n}{k}\cdot\frac{n}{d} = 2\sum_{\substack{\frac{n}{2}\neq a,\, b|\frac{n}{2} \\ \gcd(a,b)=1}} ab = 2\Phi_x\left(\frac{n}{2}\right) - 2n$$

if $l = 2$ and $i - j$ is odd and the proof is complete. □

We are now able to compute $F_2(Q_{4n})$ and $F_2(QD_{2^n})$.

THEOREM 2.2. *Let $G = Q_{4n}$ be a generalised quaternion group. Then*

$$F_2(G) = \begin{cases} F_2(D_{2n}) + 2\delta_n + 4n, & \text{odd } n, \\ F_2(D_{2n}), & \text{even } n. \end{cases}$$

*Proof.* Let $G = Q_{4n} = \langle x, y : x^{2n} = 1, x^n = y^2, x^y = x^{-1}\rangle$, $A, B \leq G$ such that $G = AB$ and $\bar{G} = G/Z(G)$. Since $1 \neq (x^i y)^2 = y^2 \in Z(G) = \langle x^n\rangle$, we have $H \leq \langle x\rangle$, which is of odd order for each subgroup $H$ of $G$ such that $H \cap Z(G) = 1$.

If $Z(G) \subseteq A, B$, then $D_{2n} \cong \bar{G} = \bar{A}\bar{B}$ and the number of solutions $(A, B)$ in this case is $F_2(D_{2n})$ and if $A \cap Z(G) = B \cap Z(G) = 1$, then $A, B \leq \langle x\rangle$, which is impossible.

In what follows we may assume without loss of generality that $Z(G) \subseteq A$ and $B \cap Z(G) = 1$. Let $\bar{B} = BZ(G)/Z(G)$. Then $D_{2n} \cong \bar{G} = \bar{A}\bar{B}$. If $\bar{A}$ is non-cyclic, then as in the proof of Theorem 2.1, the number of solutions $(A, B)$ is $\delta_n$ and if $\bar{A}$ is cyclic, then $\bar{A} \not\leq \langle \bar{x} \rangle$, which implies that $\bar{A} = \langle \bar{x}^i \bar{y} \rangle$. Thus, $A = \langle x^i y \rangle$ and $A \cap B = 1$ for $|B|$ is odd, which implies that $|G| = |A||B|$. Hence, $|B| = n$ and the number of solutions $(A, B)$ is $2n$. □

THEOREM 2.3. *Let $G = QD_{2^n}$ $(n \geq 4)$ be a quasi-dihedral group. Then,*

$$F_2(G) = F_2(D_{2^{n-1}}) + 2^n + 2^{n-1} + 2.$$

*Proof.* Let $G = QD_{2^n} = \langle x, y : x^{2^{n-1}} = y^2 = 1, x^y = x^{2^{n-2}-1} \rangle$, $A, B \leq G$ such that $G = AB$ and let $\bar{G} = G/Z(G)$. Clearly, $Z(G) = \langle x^{2^{n-2}} \rangle$.

If $Z(G) \subseteq A, B$, then $D_{2^{n-1}} \cong \bar{G} = \bar{A}\bar{B}$ and the number of solutions $(A, B)$ in this case is $F_2(D_{2^{n-1}})$, and if $A \cap Z(G) = B \cap Z(G) = 1$, then $A, B = 1$ or some $\langle x^{2i} y \rangle$. Hence, $|A|, |B| \leq 2$, which implies that $|G| \leq 4$, a contradiction.

In the sequel we may assume without loss of generality that $Z(G) \subseteq A$ and $B \cap Z(G) = 1$. If $B = 1$, then $A = G$ and we are done. Thus, we may assume that $B \neq 1$, which implies that $B = \langle x^{2i} y \rangle$ for some $i$. Then $D_{2^{n-1}} \cong \bar{G} = \bar{A}\bar{B}$, where $\bar{B} = BZ(G)/Z(G)$. If $\bar{A}$ is non-cyclic, then as in the proof of Theorem 2.1, the number of solutions $(A, B)$ is $2^{n-2} + 2^{n-2} = 2^{n-1}$, for $\bar{B} = \langle \bar{x}^{2i} \bar{y} \rangle$ and $2i$ is even. Finally, suppose $\bar{A}$ is cyclic. If $\bar{A} \leq \langle \bar{x}^j \bar{y} \rangle$, then $|\bar{G}| \leq |\bar{A}||\bar{B}| \leq 4$, which is impossible. Thus, $\bar{A} \leq \langle \bar{x} \rangle$ and consequently $A \leq \langle x \rangle$. Now we have $2^n = |G| = |A||B| = 2|A|$, which implies that $|A| = 2^{n-1}$ and consequently $A = \langle x \rangle$. Hence, the number of solutions $(A, B)$ in this case is $2^{n-2}$. □

We conclude this section by computing $F_2(G)$ for modular $p$-groups $M_{p^n}$.

THEOREM 2.4. *Let $G = M_{p^n}$ $(n \geq 3)$ be a modular $p$-group. Then*

$$F_2(G) = \begin{cases} 2(n-2)(p(p+1)+1) + p^2 + 3p + 5, & p^n \neq 8, \\ 41, & p^n = 8. \end{cases}$$

*Proof.* Let $G = M_{p^n} = \langle x, y : x^{p^{n-1}} = y^p = 1, x^y = x^{p^{n-2}+1} \rangle$ and $A, B \leq G$ such that $G = AB$. Also, let $Z = \langle x^{p^{n-2}} \rangle = \Omega_1(Z(G))$. If $p^n = 8$, then $G \cong D_8$ and $F_2(G) = 41$. Thus, we may assume that $p^n \neq 8$.

If $Z \subseteq A, B$, then $G/Z = A/Z \cdot B/Z$ and $G/Z \cong \mathbb{Z}_{p^{n-2}} \times \mathbb{Z}_p$. Hence, the number of such $(A, B)$ is $F_2(\mathbb{Z}_{p^{n-2}} \times \mathbb{Z}_p)$.

If $Z \not\subseteq A, B$, then $|A| = |B| = p$ and $|G| \leq p^2$, which is impossible. Thus, we may assume without loss of generality that $Z \subseteq A$ and $Z \not\subseteq B$. Then $|B| = p$ and $G/Z = A/Z \cdot BZ/Z$. If $B = 1$, then $A = G$. Now if $B \neq 1$, then $B = \langle x^{ip^{n-2}} y \rangle$ for $i = 0, \ldots, p-1$. Hence, the number of such $B$ is $p$. Moreover, $\exp(A) = p^{n-2}$ and if $A \neq G$, then $A/Z$ is a cyclic subgroup of $G/Z$ of order $p^{n-2}$, which is not contained in $BZ/Z$. The number of such $A$ in both cases, i.e. $n > 3$ and $n = 3$, is $p$. Hence, the number of such $(A, B)$ is $p(p+1) + 1$. Therefore, $F_2(G) = F_2(\mathbb{Z}_{p^{n-2}} \times \mathbb{Z}_p) + 2(p(p+1) + 1)$. On the other hand, by a similar discussion it can be easily shown that $F_2(\mathbb{Z}_{p^m} \times \mathbb{Z}_p) = F_2(\mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_p) + 2(p(p+1) + 1)$ for each $m > 1$ and $F_2(\mathbb{Z}_p \times \mathbb{Z}_p) = p^2 + 3p + 5$. Therefore, $F_2(G) = 2(n-2)(p(p+1)+1) + p^2 + 3p + 5$. □

COROLLARY 2.5. *If $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_p$, then*

$$F_2(G) = 2(n-1)(p(p+1)+1) + p^2 + 3p + 5.$$

https://doi.org/10.1017/S0017089511000644 Published online by Cambridge University Press

**3. Projective general and special linear groups.** We begin with recalling some well-known properties of $PSL(2,p^n)$ about the structure of $PSL(2,p^n)$ and its subgroups.

THEOREM 3.1. (Dickson's Theorem, Hauptsatz II.8.27 in [**4**]). *Any subgroup of $PSL(2,p^n)$ is isomorphic to one of the following families of groups*:

*(1) Elementary abelian p-groups.*
*(2) Cyclic groups of order m, where m is a divisor of* $(p^n \pm 1)/d$ *and* $d = \gcd(p-1, 2)$.
*(3) Dihedral groups of order 2m, where m is as defined in* (2).
*(4) Alternating group* $A_4$ *if* $p > 2$ *or* $p = 2$ *and* $n \equiv 0 \pmod 2$.
*(5) Symmetric group* $S_4$ *if* $p^{2n} \equiv 1 \pmod{16}$.
*(6) Alternating group* $A_5$ *if* $p = 5$ *or* $p^{2n} \equiv 1 \pmod 5$.
*(7) A semi-direct product of an elementary abelian p-group of order* $p^m$ *and a cyclic group of order k, where k is a divisor of* $p^m - 1$ *and* $p^n - 1$.
*(8) The group* $PSL(2,p^m)$ *if m is a divisor of n, or the group* $PGL(2,p^m)$ *if 2m is a divisor of n.*

THEOREM 3.2. (Satz II.8.5 in[**4**]). *If* $G = PSL(2,p^n)$*, then there exists subgroups* $\mathcal{H}$, $\mathcal{K}$ *and* $\mathcal{L}$ *of G such that*

$$G = \bigcup_{g\in G} \mathcal{H}^g \cup \bigcup_{g\in G} \mathcal{K}^g \cup \bigcup_{g\in G} \mathcal{L}^g,$$

*$\mathcal{H}$ is a Sylow p-subgroup of G, which is elementary abelian of order $p^n$, $\mathcal{K}$ is cyclic of order $(p^n-1)/d$ and $\mathcal{L}$ is cyclic of order $(p^n+1)/d$, where* $d = \gcd(p-1,2)$. *Moreover,* $[G : N_G(\mathcal{H})] = p^n + 1$, $[G : N_G(\mathcal{K})] = p^n(p^n+1)/2$ *and* $[G : N_G(\mathcal{L})] = p^n(p^n-1)/2$.

Note that in the above theorem, for $\mathcal{H}$, $\mathcal{K}$ and $\mathcal{L}$ we have $N_G(N_G(\mathcal{H})) = N_G(\mathcal{H})$, $N_G(N_G(\mathcal{K})) = N_G(\mathcal{K})$ and $N_G(N_G(\mathcal{L})) = N_G(\mathcal{L})$.

Ito [**5**] uses Dickson's theorem to obtain all the possible factorizations of projective special linear groups. According to Ito's results, $PSL(2,p^n) = AB$ ($p^n > 59$) is a factorization of $PSL(2,p^n)$ if and only if the order of $A$ or $B$, say $A$, is divisible by $p^n$ and

(i) $p = 2$, $A$ is conjugate to $N_G(\mathcal{H})$ and $B$ is conjugate to $\mathcal{L}$,
(ii) $p = 2$, $A$ is conjugate to $N_G(\mathcal{H})$ and $B$ is conjugate to $N_G(\mathcal{L})$ or
(iii) $p > 2$, $(p^n-1)/2$ is odd, $A$ is conjugate to $N_G(\mathcal{H})$ and $B$ is conjugate to $N_G(\mathcal{L})$.

Utilising the Ito's results we have the following.

THEOREM 3.3. *Let* $G = PSL(2,p^n)$ *be a projective special linear group. Then*

$$F_2(G) = \begin{cases} 2|L(G)| + 2p^n(p^{2n}-1) - 1, & p = 2, n > 1 \\ 2|L(G)| + p^n(p^{2n}-1) - 1, & p > 2 \text{ and } (p^n-1)/2 \text{ is odd} \\ & p^n \neq 3, 7, 11, 19, 23, 59 \\ 2|L(G)| - 1, & p > 2 \text{ and } (p^n-1)/2 \text{ is even} \\ & p^n \neq 5, 9, 29 \end{cases},$$

*and*

$$F_2(G) = 17, 27, 237, 1\,141, 2\,033, 4\,935, 17\,223, 48\,261, 68\,799, 780\,695$$

https://doi.org/10.1017/S0017089511000644 Published online by Cambridge University Press

*if*

$$p^n = 2, 3, 5, 7, 9, 11, 19, 23, 29, 59,$$

*respectively.*

*Proof.* If $p^n > 59$, then the result follows directly from (i), (ii) and (iii) and the notes after Theorem 3.2. For the case $p^n \leq 59$ we may apply GAP software [**8**] to compute the number of factorizations of $G$. □

We now consider the projective general linear groups. The methods here are essentially the same as Ito's method but with some more difficulty. As $PGL(2, 2^n) \cong PSL(2, 2^n)$ we just consider the groups $PGL(2, p^n)$ for $p$ odd. We first give correspondences to Theorems 3.1 and 3.2 for projective general linear groups. Since by Dickson's theorem $PGL(2, p^n)$ is a subgroup of $PSL(2, p^{2n})$, we have the following.

THEOREM 3.4. *Any subgroup of $PGL(2, p^n)$ is isomorphic to one of the following families of groups*:

*(1) Elementary abelian $p$-groups.*
*(2) Cyclic groups of order $m$, where $m$ is a divisor of $p^n \pm 1$.*
*(3) Dihedral groups of order $2m$, where $m$ is a divisor of $p^n \pm 1$.*
*(4) Alternating group $A_4$.*
*(5) Symmetric group $S_4$ if $p^{2n} \equiv 1 \pmod{16}$.*
*(6) Alternating group $A_5$ if $p = 5$ or $p^{2n} \equiv 1 \pmod{5}$.*
*(7) A semi-direct product of an elementary abelian $p$-group of order $p^m$ and a cyclic group of order $k$, where $k$ is a divisor of $p^m - 1$ and $p^n \pm 1$.*
*(8) The group $PSL(2, p^m)$ if $m$ is a divisor of $2n$, or the group $PGL(2, p^m)$ if $m$ is a divisor of $n$.*

THEOREM 3.5. (Satz II.8.5 in [**4**]). *If $G = PGL(2, p^n)$ $(p > 2)$, then there exists subgroups $\mathcal{H}$, $\mathcal{K}$ and $\mathcal{L}$ of $G$ such that*

$$G = \bigcup_{g \in G} \mathcal{H}^g \cup \bigcup_{g \in G} \mathcal{K}^g \cup \bigcup_{g \in G} \mathcal{L}^g,$$

*$\mathcal{H}$ is a Sylow $p$-subgroup of $G$, which is elementary abelian of order $p^n$, $\mathcal{K}$ is cyclic of order $p^n - 1$ and $\mathcal{L}$ is cyclic of order $p^n + 1$. Moreover, $[G : N_G(\mathcal{H})] = p^n + 1$, $[G : N_G(\mathcal{K})] = p^n(p^n + 1)/2$ and $[G : N_G(\mathcal{L})] = p^n(p^n - 1)/2$.*

The same as before for $\mathcal{H}$, $\mathcal{K}$ and $\mathcal{L}$ in the above theorem, we have $N_G(N_G(\mathcal{H})) = N_G(\mathcal{H})$, $N_G(N_G(\mathcal{K})) = N_G(\mathcal{K})$ and $N_G(N_G(\mathcal{L})) = N_G(\mathcal{L})$. The notations of the above theorem will be used frequently in the remaining paper.

Let $G = PGL(2, p^n)$ ($p > 2$ and $p^n > 29$) and $A, B \leq G$ such that $G = AB$. Note that by Theorem 3.5, a maximal cyclic subgroup of $G$ has order $p$, $p^n - 1$ or $p^n + 1$. Clearly the number of pairs $(A, B)$ such that $A = G$ or $B = G$ is $2|L(G)| - 1$. Hence, we may assume that $A$ and $B$ are non-trivial proper subgroups of $G$. Also if $A$ or $B$ equals to the unique subgroup $M$ of $PGL(2, p^n)$ isomorphic to $PSL(2, p^n)$, then the number of pairs $(A, B)$ equals $2(|L(G)| - |L(M)|)$. Hence, we further assume that $A, B \neq M$.

First assume that $p$ divides both $|A|$ and $|B|$. Then $A$ and $B$ are isomorphic to

(1) an elementary abelian $p$-group;

(2) $A_4$ if $p = 3$;
(3) $S_4$ if $p = 3$;
(4) $A_5$ if $p = 3$ or 5;
(5) a semi-direct product of an elementary abelian $p$-group of order $p^m$ and a cyclic group of order $k$ such that $k$ divides $p^m - 1$ and $p^n \pm 1$; or
(6) $PSL(2, p^m)$ if $m|2n$ ($m \neq 2n$) or $PGL(2, p^m)$ if $m|n$.

Since the number of pairs $(A, B)$, where $A, B$ are of a fix type equals to the number of pairs $(B, A)$, in what follows without loss of generality we assume that the type of $B$ is greater than or equal to the type of $A$.

LEMMA 3.6. *The number p does not divide both* $|A|$ *and* $|B|$.

*Proof.* If $A$ is an elementary abelian $p$-subgroup, then $p^{2n} - 1$ divides $|B|$, which is possible only if $B = G$, a contradiction.

If $A \cong A_4$, then $p = 3$, $n > 2$ and $p^{n-1}(p^{2n} - 1)/4$ divides $|B|$. Hence, $B$ is not isomorphic to any of the groups of types (2) to (5). If $B \cong PGL(2, p^m)$, then $m = n$, which is a contradiction. Also if $B \cong PSL(2, p^m)$, then either $m = 2$ and $n = 3$, which implies that

$$3^2 \cdot \frac{3^6 - 1}{4} ||B| = 3^2 \cdot \frac{3^4 - 1}{2},$$

or $m = n$ and $B = M$, which are both impossible. If $A \cong S_4$ or $A_5$, then similarly we reach to a contradiction.

Suppose that $A \cong \mathbb{Z}_p^m \rtimes \mathbb{Z}_k$, where $k$ divides $p^m - 1$ and $p^n \pm 1$. If $B \cong \mathbb{Z}_p^{m'} \rtimes \mathbb{Z}_{k'}$, where $k'$ divides $p^{m'} - 1$ and $p^n \pm 1$, then $p^{2n} - 1|kk'$, which implies that $k = p^n + 1$ and $k' = p^n - 1$, or $k = p^n - 1$ and $k' = p^n + 1$. But, then $p^n + 1$ must divides $p^m - 1$ or $p^{m'} - 1$, which is impossible. Now suppose that $B \cong PSL(2, p^{m'})$ ($m' \neq n, 2n$) or $PGL(2, p^{m'})$ ($m' \neq n$). As $k|p^n \pm 1$ we have $p^n \mp 1||B|$. Thus, $(p^n \mp 1)/2|p^{m'} \mp 1$, which is impossible.

Finally, suppose that $A \cong PSL(2, p^m)$ or $PGL(2, p^m)$. Then $B \cong PSL(2, p^{m'})$ or $PGL(2, p^{m'})$ and we should have $m + m' \geq n$. Without loss of generality we asusme that $m' \geq m$ and so $m' \geq n/2$. If $m' > n/2$, then $m' = 2n/3$ and $B \cong PSL(2, p^{2n/3})$. Thus, $p^{2n} - 1$ divides $(p^{2m} - 1)(p^{4n/3} - 1)/2$ and either $m|n$ or $m|2n$ ($m \neq n$). If $m|n$, then $m = n/3$ and $p^{2n} - 1$ divides $(p^{n/3} - 1)^2$, which is a contradiction for $\gcd(p^n - 1, p^{2n/3} - 1) = p^{2n/3} - 1$ and $\gcd(p^n - 1, p^{4n/3} - 1) = p^{2n/3} - 1$. Also if $m|2n$ but $m \nmid n$, then $m = 2n/3$ or $2n/5$ and similarly we reach to a contradiction. Therefore, $m = m' = n/2$ so that $p^{2n} - 1$ divides $(p^n - 1)^2$, which implies that $p^n = 3$, a contradiction. □

According to Lemma 3.6, $p$ does not divide both $|A|$ and $|B|$. Without loss of generality we may assume that $p \nmid |B|$. Then $p^n||A|$ and $A$ is isomorphisc to

(1′) a Sylow $p$-subgroup of $G$, or
(2′) a semi-direct product of an elementary abelian $p$-group of order $p^n$ and a cyclic group of order $k$ such that $k|p^n - 1$.

LEMMA 3.7. *A is a group of type (2′) and*

*(i) A is conjugate to $N_G(\mathcal{H})$ and B is conjugate to $\mathcal{L}$,*
*(ii) A is conjugate to $N_G(\mathcal{H})$ and B is conjugate to one of the two dihedral subgroups of $N_G(\mathcal{L})$ of index 2,*
*(iii) A is conjugate to $N_G(\mathcal{H})$ and B is conjugate to $N_G(\mathcal{L})$,*

*(iv)* *$A$ is conjugate to the unique subgroup of $N_G(\mathcal{H})$ of index 2, $B$ is conjugate to $N_G(\mathcal{L})$, $n$ is odd and $p \overset{4}{\equiv} 3$.*

*In either case, the number of pairs $(A, B)$ is $p^n(p^{2n} - 1)/2$.*

*Proof.* If $A$ is a Sylow $p$-subgroup of $G$, then $p^{2n} - 1$ divides $|B|$ and so $B = G$, a contradiction.

Now assume that $A \cong \mathbb{Z}_p^n \rtimes \mathbb{Z}_k$, where $k$ divides $p^n - 1$. Then $p^n + 1$ divides $|B|$ and $B$ is isomorphic to $A_4$, $S_4$, $A_5$, a cyclic group or a dihedral group. Clearly, $B \ncong A_4$ or $S_4$. Also, $B \ncong A_5$ for otherwise $p^n = 59$ and a simple computation with GAP software [**8**] shows that $PGL(2, 59)$ has no subgroups isomorphic to $A_5$. If $B$ is cyclic, then we should have $|B| = p^n + 1$ and hence $B$ is conjugate to $\mathcal{L}$. In this case $|A| = p^n(p^n - 1)$ and $A$ is a conjugate of $N_G(\mathcal{H})$. Finally, suppose $B$ is a dihedral group. Then $|B| = p^n + 1$ or $2(p^n + 1)$. If $|B| = p^n + 1$, then $|A| = p^n(p^n - 1)$ and so $A$ is a conjugate of $N_G(\mathcal{H})$. Also, $B$ is conjugate to a dihedral subgroup of $N_G(\mathcal{L})$. Note that $N_G(\mathcal{L})$ is a dihedral group of order $2(p^n + 1)$ and has just two dihedral subgroups of index 2, say $\langle a^2\rangle \rtimes \langle x\rangle$ and $\langle a^2\rangle \rtimes \langle ax\rangle$, where $a$ is a generator of $\mathcal{L}$. But then $|A\langle a^2\rangle| = p^n(p^{2n} - 1)/2$ and

$$G = A\langle a^2\rangle \cup A\langle a^2\rangle x$$

and

$$G = A\langle a^2\rangle \cup A\langle a^2\rangle ax,$$

from which it follows that $A\langle a^2\rangle x = A\langle a^2\rangle ax$. Hence, $Aa^{2k}x = Aax$ for some $k$ so that $a^{2k-1} \in A$. On the other hand, by Theorem 3.5, $\langle a\rangle \cap A = 1$ so that $a^{2k-1} = 1$, which is a contradiction as $|a| = p^n + 1$ is even. Now suppose that $|B| = 2(p^n + 1)$. Then $B$ is conjugate to $N_G(\mathcal{L})$ and $|A| = p^n(p^n - 1)$ or $p^n(p^n - 1)/2$. If $|A| = p^n(p^n - 1)$, then $A$ is conjugate to $N_G(\mathcal{H})$ and we are done. Thus, we may assume that $|A| = p^n(p^n - 1)/2$. Then $A$ is a maximal subgroup of $A'$ of index 2, where $A'$ is a conjugate of $N_G(\mathcal{H})$. As $G = A'B$ one gets $|A' \cap B| = 2$, from which we conclude that $|A|$ is odd, which is possible only if $n$ is odd and $p \overset{4}{\equiv} 3$. The remaining of proof is straightforward. □

Utilising the above results we have the following.

THEOREM 3.8. *Let $G = PGL(2, p^n)$ $(p > 2)$ be a projective general linear group and $M$ be a unique subgroup of $G$ isomorphic to $PSL(2, p^n)$. Then,*

$$F_2(G) = \begin{cases} 3p^n(p^{2n} - 1) + 4|L(G)| - 2|L(M)| - 3, & n \text{ even or } p \overset{4}{\equiv} 1 \\ 4p^n(p^{2n} - 1) + 4|L(G)| - 2|L(M)| - 3, & n \text{ odd and } p \overset{4}{\equiv} 3 \end{cases}$$

*if $p^n > 29$ and $F_2(G)$ equals*

177, 1103, 3 083, 4 919, 15 549, 14 529, 31 093, 58 429, 111 567, 99 527, 144 297, 192 349

*if $p^n$ equals*

3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29,

*respectively.*

*Proof.* If $p^n > 29$, then the result follows from Lemmas 3.6 and 3.7. Also if $p^n \leq 29$, then we may apply GAP software [**8**] to verify exceptional cases. □

https://doi.org/10.1017/S0017089511000644 Published online by Cambridge University Press

## REFERENCES

**1.** M. Blaum, Factorizations of the simple groups $PSL_3(q)$ and $PSU_3(q^2)$, *Arch. Math.* **40** (1983), 8–13.

**2.** T. R. Gentchev, Factorizations of the sporadic simple groups, *Arch. Math.* **47** (1986), 97–102.

**3.** T. R. Gentchev, Factorizations of the groups of Lie type of Lie rank 1 or 2, *Arch. Math.* **47** (1986), 493–499.

**4.** B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin, 1967).

**5.** N. Ito, On the factorizations of the linear fractional group $LF(2, p^n)$, *Acta Sci. Math.* (Szeged), **15** (1953), 79–84.

**6.** K. B. Tchakerian and T. R. Gentchev, Factorizations of the groups $G_2(q)$, *Arch. Math.* **44** (1985), 230–232.

**7.** M. Tărnăuceanu, Subgroup commutativity degrees of finite groups, *J. Algebra* **321**(9) (2009), 2508–2520.

**8.** The GAP Group, GAP *Algorithms and Programming, Version 4.4.12* (2008), http://www.gap-system.org/