ISRAEL JOURNAL OF MATHEMATICS 93 (1996), 345–358

ON THE POSSIBLE NUMBER OF ELEMENTS OF GIVEN ORDER IN A FINITE GROUP

BY

RÓBERT FREUD*

Eötvös University, Department of Algebra and Number Theory
H-1088 Budapest, Múzeum krt. 6–8, Hungary
e-mail: freudrobert@ludens.elte.hu

AND

PÉTER PÁL PÁLFY**

Mathematical Institute of the Hungarian Academy of Sciences
H-1364 Budapest, Pf. 127, Hungary
e-mail: ppp@math-inst.hu

ABSTRACT

The main motivation of this paper is to introduce a problem of some combinatorial flavor about finite groups which seems to be new in the literature. Let $k > 1$ be a fixed positive integer and denote by $f(k,G)$ the number of elements of order k in the group G. We examine the set $F(k) = \{f(k,G) \mid G$ a finite group$\} \setminus \{0\}$. We give a complete characterization of $F(k)$ if $4 \mid k$ or $k = 6$ and show some modest partial results for certain other values of k. It seems to us that the question is surprisingly difficult even in such simple cases as $k = 3$, which we investigate in detail.

* Research (partially) supported by Hungarian National Foundation for Scientific Research (OTKA), Grant No. 1901.

** Research (partially) supported by Hungarian National Foundation for Scientific Research (OTKA), Grant No. 1903.

Received September 12, 1994

1. Introductory remarks

Notation: As it was introduced in the Abstract, $f(k,G)$ denotes the number of elements of order k in the group G, and we will investigate the set $F(k)$ of all possible (positive) values of $f(k,G)$.

Let $s(k,G)$ denote the number of cyclic subgroups of order k in G and $r(k,G)$ the number of solutions of the equation $g^k = 1$ in G. Obviously, we have

$$f(k,G) = \varphi(k) \cdot s(k,G) \tag{1.1}$$

and

$$r(k,G) = \sum_{d|k} f(d,G). \tag{1.2}$$

In a group G the identity element will be denoted by 1, the order of the element g by $o(g)$ and we use the standard notation for the center, the centralizer, the normalizer and the commutator. The cyclic group of order r generated by c will be denoted by $C_r = \langle c \rangle$, while D_r stands for the dihedral group of order $2r$.

The greatest common divisor of a and b will be denoted by (a,b) and their least common multiple by $[a,b]$. We will let p and q_i stand for prime numbers, q for prime powers.

THE CASE $k = 2$.

PROPOSITION 1.1: *$F(2)$ is the set of all odd numbers.*

Proof: If G has an element of order 2 then $|G|$ is even, and the matching $g \mapsto g^{-1}$ forms pairs for $o(g) > 2$, $g = 1$ remains alone and so do the elements of order 2, hence the total number of the latter ones must be odd.

On the other hand the dihedral group D_{2r} or D_{2r+1} contains $2r+1$ elements of order 2 (and the cyclic group C_2 has one element of order 2). ∎

NECESSARY CONDITIONS.

PROPOSITION 1.2: *Assume that $m \in F(k)$. Then*

(i) *$\varphi(k)|m$, and*

(ii) *if $k = p$ is prime then also $m \equiv p-1 \pmod{p(p-1)}$.*

Proof: (i) follows from (1.1). (ii) is a combination of (i) and of $m \equiv -1 \pmod p$, which is a direct consequence of a famous theorem of Frobenius (see e.g. [Frob] or [Hall, page 137]): $r(n,G) \equiv 0 \pmod n$ if $n|\ |G|$. ∎

INFINITE GROUPS. We show that allowing infinite groups will leave (the finite values in) $F(k)$ unchanged:

PROPOSITION 1.3: *Assume that G is an infinite group and $f(k,G)$ is finite. Let H denote the subgroup of G generated by all elements of order k. Then H is finite.*

Proof: Obviously, $f(k,H) = f(k,G)$. Let $x_1,\ldots,x_m$ be the elements of order k in G. Since $|H\colon C_H(x_i)|$ is the number of the conjugates of x_i, and all these conjugates have order k, therefore $|H\colon C_H(x_i)| \le m$, and thus also $\bigcap C_H(x_i)$ has finite index in H. Since $x_1,\ldots,x_m$ generate H, we have $\bigcap C_H(x_i) = Z(H)$. It is well known (see [Hupp, page 417]) that $|H/Z(H)| < \infty$ implies $|H'| < \infty$. Now H/H' is an abelian group generated by $x_1H',\ldots,x_mH'$, hence $|H/H'| \le k^m$, thus H is finite, as well. ∎

2. The case $4|k$

THEOREM 2.1: *If $4|k$, then $F(k)$ consists of all multiples of $\varphi(k)$.*

Proof: In view of Proposition 1.2 we only have to show that the condition is sufficient. Consider the semidirect product G of the normal subgroup N by the subgroup $H = C_k = \langle c\rangle$ where N is the direct product of cyclic groups of prime order and the homomorphism $\rho_c\colon N \to N$ is defined by $\rho_c(n) = n^{-1}$. This means the identity $nc = cn^{-1}$ and implies

$$(c^in)^2 = \begin{cases} c^{2i}, & \text{if } i \text{ is odd;} \\ c^{2i}n^2, & \text{if } i \text{ is even.} \end{cases} \tag{2.1}$$

(A) Let i be odd and determine the order of c^in. By (2.1), this order cannot be odd (since $4|k$). On the other hand

$$(c^in)^{2s} = c^{2is} = 1 \iff k|2is \iff \frac{k}{(k,i)}\Big|2s\frac{i}{(k,i)} \iff \frac{k}{(k,i)}\Big|2s.$$

Here (k,i) is odd, and therefore $k/(k,i)$ is even, which means that $o(c^in) = k/(k,i)$. We infer that

$$o(c^in) = k \iff (k,i) = 1.$$

(B) Let now i be even. Then

$$o(c^in) = [o(c^i), o(n)] = [k/(k,i), o(n)] \neq k$$

since the exponent of 2 is smaller both in $k/(k,i)$ and in $o(n)$ than in k (the latter one comes from $4 \nmid o(n)$).

Summarizing (A) and (B) we see that $f(k,G) = \varphi(k)|N|$. Since we have no restriction on $|N|$, any multiple m of $\varphi(k)$ belongs to $F(k)$. ∎

3. The case $k = 3$

Now we consider the case when $k = p > 2$ is a prime number. We shall obtain some general results, but we can get close to the determination of $F(p)$ only for $p = 3$. We take finite groups with $p||G|$. Our analysis will differ heavily if the Sylow p-subgroups of G are cyclic or non-cyclic.

In the case $p = 3$ we shall see that the groups with cyclic Sylow 3-subgroups make a contribution to $F(3)$ only with a set of density zero (Corollary 3.3 and Lemma 3.4). On the other hand $F(3)$ has positive density, in fact we show (Theorem 3.10) that $54j + 44 \in F(3)$ for every $j = 0, 1, 2, \ldots$

As usual, let $O_{p'}(G)$ denote the largest normal subgroup of G with order not divisible by p, and $O^{p'}(G)$ the smallest normal subgroup with a factor group of order coprime to p.

LEMMA 3.1: *Let G have cyclic Sylow p-subgroups. Then $O^{p'}(G)/O_{p'}(O^{p'}(G))$ is either simple or a cyclic p-group.*

Proof: We may assume that $O^{p'}(G) = G$ and $O_{p'}(G) = 1$. Take a minimal normal subgroup $M \lhd G$. By assumption, $p||M|$. A minimal normal subgroup is the direct product of isomorphic simple subgroups. As also the Sylow p-subgroups of M are cyclic, M must be simple. We shall distinguish two cases: M is nonabelian or M is cyclic of order p. Let $P = \langle c \rangle$ be a cyclic Sylow p-subgroup of G. If $P \leq M$, then $M = G$ follows from $O^{p'}(G) = G$. So assume $P \not\leq M$.

In the first case consider the subgroup $H = MP$. Let $h = xy \in N_H(P)$ with $x \in M$, $y \in P$. Then $[h, c] = [x, c] \in M \cap P$, hence h acts trivially on $P/(M \cap P)$. Therefore h acts trivially on P, as well [Asch, 24.1], i.e. $h \in C_H(P)$. Now $N_H(P) = C_H(P)$, hence by Burnside's theorem [Asch, 39.1] there exists a normal p-complement K in H. Since K is also a normal p-complement in M, we get a contradiction with the simplicity of M.

In the second case $|M| = p$. Now $G/C_G(M)$ is cyclic of order dividing $p - 1$, hence our assumption implies $M \leq Z(G)$. Let $g \in N_G(P)$, then g acts trivially on M, and since $M = \Omega_1(P)$ (i.e. the subgroup generated by the elements of order p), g acts trivially also on P [Asch, 24.3]. Thus $N_G(P) = C_G(P)$ and Burnside's theorem again yields a normal p-complement K in G. As $O_{p'}(G) = 1$, we have $K = 1$ and $G = P$. ∎

As $f(p,G) = f(p,O^{p'}(G))$, we may assume without loss of generality that $O^{p'}(G) = G$, i.e. G has no proper p'-factor groups. Now $G/O_{p'}(G)$ is either simple or cyclic of order p^k, $k \geq 2$. In the latter case let P be a subgroup of order p. Then $f(p,G) = f(p,O_{p'}(G) \cdot P)$, hence we may also assume without loss of generality that $G/O_{p'}(G)$ is simple, including the case $|G/O_{p'}(G)| = p$. Now we should analyse the action of G on the chief factors of $O_{p'}(G)$. Instead, we shall take into account the action of $N_G(P)$ only, thereby obtaining necessary conditions for $f(p,G)$.

LEMMA 3.2: *Let G be a finite group with cyclic Sylow p-subgroups and let P denote a subgroup of order p. Assume that $G/O_{p'}(G)$ is simple. Write*

$$\frac{f(p,G)}{f(p,G/O_{p'}(G))} = q_1^{\alpha_1} \dots q_r^{\alpha_r}.$$

Then

(i) *p divides each $q_i^{\alpha_i} - 1$, and*
(ii) *$|N_G(P): C_G(P)|$ divides each α_i.*

Proof: Let us denote $N = O_{p'}(G)$. Grouping the elements of order p in G which generate the same subgroup modulo N we obtain

$$f(p,G) = \frac{f(p,G/N)}{p-1} \cdot f(p,NP),$$

since any subgroup of order p is conjugate to P in G. Furthermore, we have

$$f(p,NP) = (p-1) \cdot |NP: N_{NP}(P)| = (p-1) \cdot |N: C_N(P)|,$$

as $N_{NP}(P) = P \times C_N(P)$. Now let q_i be an arbitrary prime divisor of $|N|$. Let us choose a Sylow q_i-subgroup Q_i of $C_N(P)$. By well-known results on coprime action [Asch, 18.7] Q_i is contained in a P-invariant Sylow q_i-subgroup R_i of N. So we have

$$|N: C_N(P)| = \prod |R_i: Q_i|,$$

where $|R_i\colon Q_i| = q_i^{\alpha_i}$. Now $Q_i = R_i \cap C_N(P)$, so P permutes the elements of $R_i \setminus Q_i$ in cycles of length p, hence $p|(|R_i| - |Q_i|) = |Q_i|(q_i^{\alpha_i} - 1)$, and so (i) follows.

Furthermore, notice that $N_G(P)/C_G(P)$, being isomorphic to a group of automorphisms of the p-element cyclic group P, is cyclic, and choose an element x such that $N_G(P) = \langle x, C_G(P)\rangle$. Now R_i^x is also P-invariant, as $P^x = P$. Hence another part of the Coprime Action Theorem [Asch, 18.7.2] yields an element $y \in C_N(P)$ such that $R_i^{xy} = R_i$. We have that Q_i^{xy} is centralized by $P^{xy} = P$, so $Q_i^{xy} \leq R_i \cap C_N(P) = Q_i$, hence we have equality here. As $\langle xy, C_G(P)\rangle = \langle x, C_G(P)\rangle$ we can replace x by xy and assume that $Q_i^x = Q_i$ and $R_i^x = R_i$. Now let us take a maximal chain of subgroups $Q_i = X_0 \lhd X_1 \lhd \cdots \lhd X_{k-1} \lhd X_k = R_i$, such that each X_j is both P- and x-invariant. Then each factor X_j/X_{j-1} is an elementary abelian q_i-group, $\langle P, x\rangle$ acts irreducibly on X_j/X_{j-1} and the action of P is fixed-point-free on X_j/X_{j-1} [Asch, 18.7.4]. Let g be a generator of P. Consider the characteristic polynomial $\kappa(x)$ of the linear transformation induced by g on X_j/X_{j-1}. Its zeroes are some primitive p-th roots of unity. Since $g^x = g^m$ (for some $1 \leq m \leq p-1$) has the same characteristic polynomial as g, it follows that $\epsilon, \epsilon^m, \epsilon^{m^2}, \ldots$ occur with the same multiplicities as zeroes of $\kappa(x)$. Since their number is $|N_G(P)\colon C_G(P)|$ we get that $|N_G(P)\colon C_G(P)|$ divides $\deg \kappa(x) = \dim X_j/X_{j-1}$, hence it divides $\alpha_i = \sum_{j=1}^k \dim X_j/X_{j-1}$, as well. ∎

Now we specialize Lemma 3.2 for $p = 3$.

Corollary 3.3: *Let G be a finite group with cyclic Sylow 3-subgroups. Then either $f(3,G) = 2q_1^{\alpha_1}\ldots q_r^{\alpha_r}$, where $q_i^{\alpha_i} \equiv 1 \pmod 3$ are prime powers, or $f(3,G) = n^2 f(3,S)$, where S is a nonabelian simple group with cyclic Sylow 3-subgroups and $3 \nmid n$.*

Proof: We assume $O^{3'}(G) = G$. If $G/O_{3'}(G)$ is cyclic then $f(3,G) = f(3,C_3)\cdot q_1^{\alpha_1}\ldots q_r^{\alpha_r}$, and Lemma 3.2(i) yields the desired result. If $G/O_{3'}(G) \cong S$ is a nonabelian simple group, then $f(3,G) = f(3,S)q_1^{\alpha_1}\ldots q_r^{\alpha_r}$, where $|N_G(P)\colon C_G(P)|$ divides each α_i by Lemma 3.2(ii). If $|N_G(P)\colon C_G(P)| = 2$, then we get the announced result. So suppose $N_G(P) = C_G(P)$. Let $\hat{P}$ be a (cyclic) Sylow 3-subgroup of G containing P. Then $\hat{P} \leq C_G(\hat{P}) \leq N_G(\hat{P}) \leq N_G(P) = C_G(P)$, so each element of $N_G(\hat{P})$ induces an automorphism of p'-order on $\hat{P}$ that acts trivially on $P = \Omega_1(\hat{P})$. Then $N_G(\hat{P})$ acts trivially on $\hat{P}$, as well [Asch, 24.3].

Now Burnside's Normal p-Complement Theorem [Asch, 39.1] yields that G has a normal 3-complement, contradicting to $G/O_{3'}(G) \cong S$, a nonabelian simple group. ∎

It is not hard to determine all finite simple groups with cyclic Sylow 3-subgroups using the classification of finite simple groups. We can calculate $f(3, G)$, as well.

LEMMA 3.4: *The following is a complete list of nonabelian simple groups with nontrivial cyclic Sylow 3-subgroups:*

(a) $G = \mathrm{PSL}(2, q)$, $q \equiv 2 \pmod 3$, *with* $f(3, G) = (q-1)q$;
(b) $G = \mathrm{PSL}(2, q)$, $q \equiv 1 \pmod 3$, *with* $f(3, G) = q(q+1)$;
(c) $G = \mathrm{PSL}(3, q)$, $q \equiv 2 \pmod 3$, *with* $f(3, G) = (q^3-1)q^3$;
(d) $G = \mathrm{PSU}(3, q^2)$, $q \equiv 1 \pmod 3$, *with* $f(3, G) = q^3(q^3+1)$;
(e) $G = J_1$, *the first Janko group, with* $f(3, G) = 5852 = 76 \cdot 77$.

Proof: We should go through the list of finite simple groups. Among the alternating groups A_6 already has non-cyclic Sylow 3-subgroups, and $A_5 \cong \mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5)$ need not be listed. For the sporadic groups we have consulted the [Atlas] and obtained (e). For groups of Lie type one is easily led to groups of low rank, and a detailed study — which is not presented here — yields the groups (a) – (d).

As far as $f(3, G)$ is concerned, we restrict ourselves to show the computation in the easier cases (a) and (b). Since, obviously, $f(3, \mathrm{PSL}(2,q)) = f(3, \mathrm{SL}(2,q))$, we will work in the latter group.

(a) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ and E be the unit matrix. We claim that $o(A) = 3$ iff the characteristic polynomial $\kappa_A(x) = x^2 + x + 1$.

If $\kappa_A(x) = x^2+x+1$, then clearly $A \neq E$ but $A^3 - E = (A^2+A+E)(A-E) = 0$, hence $o(A) = 3$. Conversely assume $o(A) = 3$. If $A = vE$ with a scalar $v \in \mathrm{GF}(q)$, then $E = A^3 = v^3 E$, i.e. $v^3 = 1$ which gives $v = 1$, since the order of the multiplicative group of $\mathrm{GF}(q)$ is not divisible by 3, as $q \equiv 2 \pmod 3$. Hence $A \neq vE$, thus the minimal polynomial $\mu_A(x)$ has degree 2 and so $\kappa_A(x) = \mu_A(x)$. Then we have $\kappa_A(x) | x^3 - 1 = (x-1)(x^2+x+1)$. Here x^2+x+1 is irreducible over $\mathrm{GF}(q)$, since otherwise it would have a root $v \in \mathrm{GF}(q)$ satisfying $v^3 = 1$ but $v \neq 1$. Therefore only $\kappa_A(x) = x^2 + x + 1$ is possible.

Now $\kappa_A(x) = x^2 - (a+d)x + ad - bc = x^2 + x + 1$ means $a + d = -1$ and $ad - bc = 1$. We have q ways to choose the value of a, and then d is uniquely determined. Now $bc = ad - 1 \neq 0$, since this would yield $a^2 + a + 1 = 0$. Therefore we have $q-1$ ways to choose $b \neq 0$ and then c is uniquely determined. This means that $f(3,G) = q(q-1)$.

(b) We claim again that $o(A) = 3$ iff the characteristic polynomial $\kappa_A(x) = x^2 + x + 1$, though we have to modify our arguments. Now the order of the multiplicative group in $\mathrm{GF}(q)$ is divisible by 3, hence $x^3 - 1$ has three different roots in $\mathrm{GF}(q)$, namely $1, v_1$ and v_2, and so $x^2 + x + 1 = (x - v_1)(x - v_2)$. Since $A = v_i E$ has determinant different from 1, and also $\kappa_A(x) = (x-1)(x-v_i)$ would yield determinant $v_i \neq 1$, hence only $\kappa_A(x) = x^2 + x + 1$ is possible indeed. The converse is the same as in (a).

Thus we have again $a + d = -1$ and $ad - bc = 1$. There are two possibilities for $a + d = -1$ and $ad = 1$, namely $a = v_1, d = v_2$ or vice versa. In this case $b = 0$ and c is arbitrary, or $c = 0$ and $b \neq 0$ is arbitrary, which means $2(2q-1)$ choices for A. In the other cases $bc \neq 0$, and we can argue as in (a): we obtain $(q-2)(q-1)$ further possibilities for A. This gives a total of $q(q+1)$ as stated. ∎

Note that for larger primes p there are many more types of simple groups with cyclic Sylow p-subgroups and $|N_G(P){:}\ C_G(P)|$ can assume several values, as well.

The conditions in Lemma 3.2 and Corollary 3.3 are necessary, but by no means sufficient. Nevertheless, we can construct some examples.

EXAMPLE 3.5: *Let p be a prime, $q_i^{\alpha_i}$ $(i = 1, \ldots, r)$ prime powers such that $q_i^{\alpha_i} \equiv 1 \pmod p$. Then there exists a group G with $f(p,G) = (p-1)q_1^{\alpha_1} \ldots q_r^{\alpha_r}$.*

Proof: Let N be the direct product of the additive groups of the fields $\mathrm{GF}(q_i^{\alpha_i})$. Let ϵ_i be a primitive p-th root of unity in $\mathrm{GF}(q_i^{\alpha_i})$, which exists by $p | q_i^{\alpha_i} - 1$. Let G be the semidirect product of N by a cyclic group $\langle g \rangle$ of order p, where g acts on $\mathrm{GF}(q_i^{\alpha_i})$ as a multiplication by ϵ_i. Then every element in $G \setminus N$ has order p, hence $f(p,G) = (p-1)|N|$. ∎

EXAMPLE 3.6: *For each n not divisible by 3, there exists a finite group G with $G/O_{3'}(G) \cong A_5$ and $f(3,G) = n^2 f(3, A_5) = 20n^2$.*

Proof: Let $G = C_n \wr A_5$. This wreath product is a semidirect product of C_n^5 by A_5 with the obvious action. For $P = \langle (123) \rangle$ and $N = C_n^5$ we see that $C_N(P) = \{(a,a,a,b,c) |\ a,b,c \in C_n\}$, hence $f(3,G) = f(3,G/N) \cdot |N{:}\ C_N(P)| = f(3,A_5) \cdot n^2 = 20n^2$. ∎

REMARK 3.7: *There is no finite group with $f(3,G) = 1760 = 4^2 f(3, \mathrm{PSL}(2,11))$.*

Proof: Later (Lemma 3.8) we shall see that for groups with non-cyclic Sylow 3-subgroups we have $f(3,G) \equiv -1 \pmod 9$, hence any group with $f(3,G) = 1760$ must have cyclic Sylow 3-subgroups. As we have already observed, we may assume without loss of generality that $G/O_{3'}(G)$ is simple. If $|G/O_{3'}(G)| = 3$, then $f(3,G) = 2q_1^{\alpha_1} \dots q_r^{\alpha_r}$ with $q_i^{\alpha_i} \equiv 1 \pmod 3$, which is not the case as $1760 = 2 \cdot 2^4 \cdot 5 \cdot 11$. If $G/O_{3'}(G) \cong S$, a nonabelian cyclic group, then in virtue of Corollary 3.3, $f(3,G) = n^2 f(3,S)$ for some $n \geq 1$. Now $n = 1, 2$, or 4 and $f(3,S) = 1760, 440$, or 110, correspondingly. Checking the list in Lemma 3.4 we see that only $f(3,S) = 110, n = 4$ can occur and then $S \cong \mathrm{PSL}(2,11)$. Using the notation of Lemma 3.2 we see that $|N \colon C_N(P)| = 16$. If Q is a Sylow 2-subgroup of $C_N(P)$ and R is a P-invariant Sylow 2-subgroup of N containing Q, then we obtain that $|R \colon Q| = 16$. For $H = N_G(R)$ the Frattini argument [Asch, 6.2] yields $G = NH$. Since $f(3,H) = |(N \cap H) \colon C_{N \cap H}(P)| \cdot f(3, H/(N \cap H)) = f(3,G)$, as $R \leq N \cap H$, $P \leq H$ and $H/(N \cap H) \cong NH/N = G/N$, we get $H \geq O^{3'}(G) = G$, i.e. $H = G$, so $R \lhd G$. Take a chief series $1 = X_0 \lhd X_1 \lhd \cdots \lhd X_{k-1} \lhd X_k = R \lhd \cdots$ of G. Since P does not act trivially on R, there must be at least one chief factor $V = X_j/X_{j-1}$ such that P does not act trivially on V. Then $|V \colon C_V(P)| \leq |R \colon C_R(P)| = |R \colon Q| = 16$. Now $C_G(V)$ does not contain P, hence $C_G(V) \leq O_{3'}(G) = N$. Observe that $\mathrm{PSL}(2,11)$ can be generated by two elements of order 3, and choose a $P_1 \leq G$ of order 3 such that $\langle P, P_1 \rangle N = G$. Then

$$|V \colon C_V(\langle P, P_1 \rangle)| = |V \colon (C_V(P) \cap C_V(P_1))| \leq |V \colon C_V(P)| \cdot |V \colon C_V(P_1)| \leq 16^2.$$

Let $x \in \langle P, P_1 \rangle$ be an element such that xN has order 11 in $G/N \cong \mathrm{PSL}(2,11)$. Then x acts nontrivially on V, hence 11 divides $|V| - |C_V(x)| > 0$, so it divides $|V \colon C_V(x)| - 1 > 0$, as well. Since $|V \colon C_V(x)| \leq |V \colon C_V(\langle P, P_1 \rangle)| \leq 2^8$, we get a contradiction, as the order of 2 mod 11 is 10. ∎

From Corollary 3.3 and Lemma 3.4 we see that the values $f(3,G)$ for groups G with cyclic Sylow 3-subgroups constitute a sequence of density zero. We will see that groups with non-cyclic Sylow 3-subgroups provide examples for a sequence of positive density.

Now we turn to groups with non-cyclic Sylow p-subgroups, for which a necessary condition more restrictive than Proposition 1.2(ii) holds, see Herzog [Herz, Thm. 3(c)].

LEMMA 3.8: *Let G be a finite group with non-cyclic Sylow p-subgroups, $p > 2$. Then $f(p, G) \equiv -1 \pmod{p^2}$.*

Now we restrict our attention to $p = 3$. By Lemma 3.8 and Proposition 1.2(ii) we have that for groups G with non-cyclic Sylow 3-subgroups only $f(3, G) \equiv 8 \pmod{18}$ is possible. We show that (at least) one third of these numbers do occur in $F(3)$ indeed.

Let $\mathcal{E}$ denote the set of positive integers m such that each prime $\equiv 2 \pmod 3$ occurs at an even exponent in the canonical form of m and 3 does not divide m. So $\mathcal{E} = \{1, 4, 7, 13, 16, 19, 25, 28, \ldots\}$. In virtue of Example 3.5 for each $u \in \mathcal{E}$ there exists a group G with $f(3, G) = 2u$.

LEMMA 3.9: *Let $u, v \in \mathcal{E}$. Then there exists a group G with $f(3, G) = 18(u + v) + 8$.*

Proof: As in the proof of Example 3.5, let U and V be abelian groups of order u and v, resp. with fixed-point-free automorphisms α and β of order 3. Let S be the Sylow 3-subgroup of S_9 generated by the permutations $a = (123)$ and $b = (147)(258)(369)$. Take the homomorphism ρ: $S \to \mathrm{Aut}(U \times V)$ defined by $\rho_a(xy) = \alpha(x)y$, $\rho_b(xy) = x\beta(y)$ for $x \in U$, $y \in V$. Now let G be the semidirect product of $U \times V$ by S with respect to ρ.

Here S contains 44 elements of order 3, namely 8 elements in the commutator subgroup S', 18 elements in $\langle a, S'\rangle \setminus S'$ and another 18 elements in $\langle b, S'\rangle \setminus S'$. If $c \in S$ is an element of order 3, then the number of elements of order 3 in the coset $(U \times V)c$ is $|(U \times V) : C_{U\times V}(c)|$, and this index is 1, u or v, according to the three cases listed above. Hence we have $f(3, G) = 8 + 18u + 18v$, as claimed. ∎

THEOREM 3.10: *For all $j \geq 0$, $54j + 44 \in F(3)$.*

Proof: The theorem will immediately follow from Lemma 3.9, if we can show that every number $r = 3j + 2$ ($j \geq 0$) can be written as a sum $r = u + v$ with $u, v \in \mathcal{E}$. By a result of Liouville every positive integer can be represented in the form $x^2 + y^2 + 3z^2 + 3t^2$ (see [Liou] or [Kloo, p. 459]). Let $r = x^2 + y^2 + 3z^2 + 3t^2$ and write $u = x^2 + 3z^2$, $v = y^2 + 3t^2$. As $r \equiv 2 \pmod 3$, it follows that $u \equiv 1 \pmod 3$ and $v \equiv 1 \pmod 3$. Finally, we can check easily that $u, v \in \mathcal{E}$ by observing that -3 is a quadratic non-residue modulo any odd prime congruent to 2 mod 3. ∎

Unfortunately, we were unable to prove a similar general result for the numbers of the form $54j + 8$, for example we do not know whether or not $f(3, G) = 1412$ can occur. If all these numbers belong to $F(3)$, then so do the numbers $54j + 26$, as well, since by $f(3, H \times C_3) = 3f(3, H) + 2$ we could get examples for these indeed.

We can summarize our results about $F(3)$, as follows:

SUMMARY 3.11: *Apart from a set of density zero, $F(3)$ can contain only numbers of the form $18i + 8$. Among these, all numbers of the form $54j + 44$ do belong to $F(3)$ indeed, whereas we are uncertain about the other ones.*

Finally we make a few numerical remarks.

I. A complete list of all elements in $F(3)$ less than 500 is the following: All numbers of the form $6t + 2$, *except* 68, 92, 140, 164, 176, 212, 230, 236, 284, 290, 308, 356, 374, 410, 428, 452, 464 and 470.

II. We could extend the list up to 2000, except for the dubious behavior of 1412, already mentioned. In checking whether or not some $m \leq 2000$ belongs to $F(3)$, the discussed methods were generally sufficient, we had to use a slightly different technique only for the construction of groups G with $f(3, G) = 710$, 1520 and 1790.

4. The case $k = 6$

From Proposition 1.2(i) we know that only even numbers m can belong to $F(6)$. We give now several constructions which show that all even numbers except 4, 16 and 28 do belong to $F(6)$. Some of these constructions can be easily generalized for arbitrary $F(k)$ where $k = 2p$, or even more generally $k \equiv 2 \pmod 4$.

EXAMPLE 4.1: *$m = 4j + 2 \in F(6)$ for $j \geq 0$.*

Proof: For $G = D_{2j+1} \times C_3$ we have $f(6, G) = 4j + 2$ if $j > 0$ and $f(6, C_6) = 2$. ∎

EXAMPLE 4.2: *$m = 12j \in F(6)$ for $j \geq 1$.*

Proof: For $G = D_{6j-3} \times D_3$ we have $f(6, G) = (6j - 3)2 + 3 \cdot 2 = 12j$ if $j > 0$. ∎

EXAMPLE 4.3: *$m = 12j + 8 \in F(6)$ for $j \geq 0$.*

Proof: For $G = D_{6j} \times C_3$ we have $f(6, G) = 12j + 8$ if $j > 0$. Also, $f(6, C_6 \times C_3) = 8$. ∎

This means that only the numbers $m = 12j + 4$ are left.

EXAMPLE 4.4: *$m = 24j + 52 \in F(6)$ for $j \geq 0$.*

Proof: Let S be the central product of D_4 and C_4

$$S = \langle x, y, z \mid x^4 = y^2 = 1, z^2 = x^2, yxy = x^{-1}, xz = zx, yz = zy \rangle,$$

take the semidirect product H of the normal subgroup $C_{6j+3} = \langle c \rangle$ by the subgroup S, where $c^x = c^y = c, c^z = c^{-1}$, and let $G = C_3 \times H$ with $C_3 = \langle d \rangle$.

Then each element of G has a unique representation

$$uz^k c^i d^n, \quad u \in D_4 = \langle x, y \rangle, \quad k = 0, 1, \quad 0 \leq i \leq 6j + 2, \quad 0 \leq n \leq 2.$$

If $k = 0$, then we are in $K = D_4 \times C_{6j+3} \times C_3$ and $f(6, K) = 5 \cdot 8$.

If $k = 1$, then $(uzc^i)^2 = u^2 z^2 = u^2 x^2 \in D_4$, which shows that the order of uzc^i cannot be 3 or 6. Hence $o(uzc^i d^n) = 6$ iff $o(uzc^i) = 2$ and $o(d^n) = 3$. This is equivalent to $u^2 x^2 = 1$, i.e. $u = x$ or x^3 and i is arbitrary, $n \neq 0$. This yields $2 \cdot (6j + 3) \cdot 2$ elements.

Hence we have $f(6, G) = 5 \cdot 8 + 2 \cdot (6j + 3) \cdot 2 = 24j + 52$. ∎

EXAMPLE 4.5: *$m = 48j + 40 \in F(6)$ for $j \geq 0$.*

Proof: For $G = C_3 \times C_3 \times D_{6j+5}$ we have $f(6, G) = 8(6j + 5)$. ∎

EXAMPLE 4.6: *$m = 48j + 64 \in F(6)$ for $j \geq 0$.*

Proof: Let $D_8 = \langle x, y \mid x^8 = y^2 = 1, yxy = x^{-1} \rangle$, take the semidirect product H of the normal subgroup $C_{6j+3} = \langle c \rangle$ by the subgroup D_8, where $c^x = c^{-1}, c^y = c$, and let $G = C_3 \times H$. Counting as in Example 4.4, we obtain $f(6, G) = 5 \cdot 8 + 4 \cdot (6j + 3) \cdot 2 = 48j + 64$. ∎

Now we are going to show that the remaining values $k = 4, 16, 28$ cannot occur as $f(6, G)$. In order to do this we define a bipartite graph with vertices representing the 2- and 3-element subgroups of G, and G_2 of order 2 and G_3 of order 3 are joined by an edge iff they are contained in a 6-element cyclic subgroup, i.e. iff G_2 and G_3 commute. The number of vertices adjacent to a given G_2 is exactly the number of 3-element subgroups in $C_G(G_2)$, therefore it is either 0 (and G_2 is an isolated point in the graph), or it is congruent to 1 modulo 3. Similarly, the degree of a vertex G_3 ($|G_3| = 3$) is either 0, or an odd number. Moreover, if we take an element $g \in G_3$, then the conjugation by g induces an automorphism of the graph. This automorphism fixes G_3 and all vertices adjacent to it, since these represent 2-element subgroups commuting with $G_3 = \langle g\rangle$. On the other hand, 2-element subgroups $\langle t\rangle$ not joined to $\langle g\rangle$ are not fixed by this automorphism, as $\langle g^{-1}tg\rangle \neq \langle t\rangle$. Thus the degree of $\langle g\rangle$ is congruent modulo 3 to the number of vertices representing 2-element subgroups.

Let us introduce some notation. Let the number of non-isolated vertices representing subgroups of order 2 and 3 be denoted by w and h, resp. and their degrees be $d^{(1)},\ldots,d^{(w)}$, and $d_{(1)},\ldots,d_{(h)}$. The total number of edges will be denoted by E. So we have

$$\sum_{i=1}^{w} d^{(i)} = \sum_{j=1}^{h} d_{(j)} = E = \frac{1}{2}f(6,G),$$

since each cyclic subgroup of order 6 contains exactly two elements of order 6.

Summarizing the above considerations, we have

$$\begin{aligned} d^{(i)} &\equiv 1 \pmod 3 \quad i=1,\ldots,w,\\ d_{(j)} &\equiv 1 \pmod 2 \quad j=1,\ldots,h,\\ w-d_{(j)} &\equiv 0 \pmod 3 \quad j=1,\ldots,h. \end{aligned}$$

It follows that

$$E=\sum_{i=1}^{w} d^{(i)} = w+\sum_{i=1}^{w}(d^{(i)}-1)\equiv w\equiv d_{(j)} \pmod 3,$$

therefore

$$E=\sum_{j=1}^{h} d_{(j)} \equiv hE \pmod 3 \qquad \text{and} \qquad E\equiv h \pmod 2.$$

We want to consider cases $f(6,G)\equiv 4 \pmod{12}$, i.e. $E\equiv 2 \pmod 6$. Then the previous congruences yield

$$h\equiv 1(3),\quad h\equiv 0(2),\quad d_{(j)}\equiv 2(3),\quad d_{(j)}\equiv 1(2),$$

so $h\equiv 4(6)$ and $d_{(j)}\equiv 5(6)$ for each $j=1,\ldots,h$. Thus

$$f(6,G)=2E=2\sum_{j=1}^{h} d_{(j)} \geq 2h\cdot 5\geq 2\cdot 4\cdot 5=40.$$

Therefore $4,16,28\notin F(6)$.

So we have proved:

THEOREM 4.7: *$m \in F(6) \iff 2|m$ and $m \neq 4, 16, 28$.*

ACKNOWLEDGEMENT: The authors are grateful to Antal Balog for calling their attention to some useful references.

References

[Asch] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, 1986.

[Atlas] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[Frob] G. Frobenius, *Über einen Fundamentalsatz der Gruppentheorie*, Berliner Ber. 1903, 987–991.

[Hall] M. Hall Jr., *The Theory of Groups*, 2nd ed., Chelsea, New York, 1976.

[Herz] M. Herzog, *Counting group elements of order p modulo p^2*, Proceedings of the American Mathematical Society **66** (1977), 247–250.

[Hupp] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[Kloo] H. D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta Mathematica **49** (1926), 407–464.

[Liou] J. Liouville, *Sur la représentation des nombres par la forme quadratique $x^2 + ay^2 + bz^2 + abt^2$*, Journal de Mathématiques Pures et Appliquées (2) **1** (1856), 230.