involve
a journal of mathematics

On three questions concerning groups with perfect order subsets

Lenny Jones and Kelly Toppin

mathematical sciences publishers

2011 vol. 4, no. 3

INVOLVE 4:3(2011)

On three questions concerning groups with perfect order subsets

Lenny Jones and Kelly Toppin

(Communicated by Kenneth S. Berenhaut)

In a finite group, an *order subset* is a maximal set of elements of the same order. We discuss three questions about finite groups G having the property that the cardinalities of all order subsets of G divide the order of G. We provide a new proof to one of these questions and evidence to support answers to the other two questions.

1. Introduction

Let G be a finite group. Carrie E. Finch and the first author [Finch and Jones 2002; 2003] defined the *order subset of G determined by $x \in G$* to be the set of elements in G with the same order as x. They defined G to have *perfect order subsets* — in short, to be a *POS group* — if the number of elements in each order subset of G divides the order $|G|$. It is easy to see that any nontrivial POS group has even order.

The next three theorems, whose proofs are given in [Finch and Jones 2002], allow us to refine the search for abelian POS groups to a particular class of groups.

Theorem 1.1. *Let $G \simeq (\mathbb{Z}_{p^a})^t \times M$ and $\widehat{G} \simeq (\mathbb{Z}_{p^{a+1}})^t \times M$, where M is an abelian group and p is a prime not dividing $|M|$. If G is a POS group, then so is $\widehat{G}$.*

Theorem 1.2. *Suppose $G \simeq \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_{s-1}}} \times (\mathbb{Z}_{p^{a_s}})^t \times M$, where M is an abelian group, p is a prime not dividing $|M|$, and $a_1 \le a_2 \le \ldots \le a_{s-1} < a_s$. If G is a POS group, then so is $\widehat{G} \simeq (\mathbb{Z}_{p^{a_s}})^t \times M$.*

Theorem 1.3. *If G is a POS group with $G \simeq (\mathbb{Z}_{p^a})^t \times M$, where M is an abelian group and p is a prime not dividing $|M|$, then $\widehat{G} \simeq (\mathbb{Z}_p)^t \times M$ is also a POS group.*

The previous theorems provide motivation for the following definition.

Definition 1.4. Let $G \simeq (\mathbb{Z}_2)^t \times M$, where $|M|$ is odd, be a POS group. We say that G is *minimal* if $(\mathbb{Z}_2)^t \times \widehat{M}$ is not a POS group for any subgroup $\widehat{M}$ of M.

MSC2000: primary 20F99, 11Y05; secondary 11A51.

Keywords: perfect order subsets, abelian group, symmetric group.

Theorem 1.5 [Finch and Jones 2002]. *Let $G \cong (\mathbb{Z}_2)^t \times M$, where $t \geq 1$ and M is a cyclic group of odd square-free order. If G is a POS group and $G \cong (\mathbb{Z}_2)^t \times \widehat{M}$ is not a POS group for any subgroup $\widehat{M}$ of M, then G is isomorphic to one of*

$$\begin{aligned}
&\mathbb{Z}_2,\\
&(\mathbb{Z}_2)^2 \times \mathbb{Z}_3,\\
&(\mathbb{Z}_2)^3 \times \mathbb{Z}_3 \times \mathbb{Z}_7,\\
&(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5,\\
&(\mathbb{Z}_2)^5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31},\\
&(\mathbb{Z}_2)^8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17},\\
&(\mathbb{Z}_2)^{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257},\\
&(\mathbb{Z}_2)^{17} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{131071},\\
&(\mathbb{Z}_2)^{32} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257} \times \mathbb{Z}_{65537}.
\end{aligned}$$

Various authors have investigated nonabelian groups in search of POS groups. For example, certain special linear groups were considered in [Finch and Jones 2003], the dihedral groups in [Libera and Tlucek 2003], and certain semidirect products and the alternating groups in [Das 2009]. In this article, our focus will be on the symmetric groups and on certain abelian groups, and specifically on three questions posed in [Finch and Jones 2002]:

Question 1.6. *Is S_3 the only symmetric group that is a POS group*?

Question 1.7. *If G is a POS group and $|G|$ is not a power of* 2, *then must $|G|$ be divisible by* 3?

Question 1.8. *Are there only finitely many minimal POS groups that contain noncyclic Sylow p-subgroups of odd order*?

Tuan and Hai [2010] answered Question 1.6 in the affirmative. We provide here an alternative proof that is shorter and more direct. The techniques used in our proof are similar to those of Tuan and Hai, but whereas they use a theorem of Chebyshev [1852], we resort to a more refined version of that result [Nagura 1952].

Walter Feit (personal communication; see also [Finch and Jones 2003]) answered Question 1.7 in the negative, by providing counterexamples: if p is a Fermat prime, the Frobenius group of order $p(p-1)$, with Frobenius complement $\mathbb{Z}_{p-1}$ and Frobenius kernel $\mathbb{Z}_p$, is a POS group but its order is not divisible by 3. Other counterexamples to Question 1.7 were constructed in [Das 2009].

All these counterexamples are nonabelian. This leads to a modified version of the question, for which we will show evidence of an affirmative answer:

Question 1.9 (modified Question 1.7). *If G is an abelian POS group and $|G|$ is not a power of* 2, *then must $|G|$ be divisible by* 3?

Concerning Question 1.8, the only known abelian POS group with a noncyclic Sylow p-subgroup is

$$(\mathbb{Z}_2)^{11} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times (\mathbb{Z}_{11})^2 \times \mathbb{Z}_{23} \times \mathbb{Z}_{89}, \tag{1-1}$$

found in [Finch and Jones 2002]. Theorem 4.3 below shows that this is, in fact, the only such POS group whose order has exactly 5 distinct odd prime divisors and exactly one odd square prime factor.

To summarize, these are the main results of this paper:

Theorem 1.10. *The symmetric group S_n is a POS group if and only if $n \leq 3$.*

Theorem 1.11. *Suppose that G is an abelian POS group and $|G|$ is not a power of 2. If $|G|$ is not divisible by 3, then $|G| > 4.48 \cdot 10^{457008}$, and $|G|$ has at least 57097 distinct prime factors.*

Theorem 1.12. *Let G be a minimal abelian POS group such that*

$$G \simeq (\mathbb{Z}_2)^t \times \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_{k-1}} \times (\mathbb{Z}_{p_k})^2 \times \mathbb{Z}_{p_{k+1}} \times \cdots \times \mathbb{Z}_{p_m},$$

where $p_1 < p_2 < \cdots < p_m$ are odd primes. If $1 \leq m \leq 5$, then

$$G \simeq (\mathbb{Z}_2)^{11} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times (\mathbb{Z}_{11})^2 \times \mathbb{Z}_{23} \times \mathbb{Z}_{89}.$$

2. The proof of Theorem 1.10

The proof is based on a result of Nagura, which refines a theorem of Chebyshev [1852] (also known as Bertrand's postulate) to the effect that for every integer $x \geq 4$, there exists a prime p such that $x < p < 2x - 2$.

Theorem 2.1 [Nagura 1952]. *If $x \geq 25$, then there exists a prime p such that*

$$x < p < \tfrac{6}{5}x.$$

Proof of Theorem 1.10. It is easy to verify that S_n is a POS group when $n \leq 3$. Suppose that $n \geq 60$. By Theorem 2.1, there exists a prime p such that $\frac{5}{12}n < p < \frac{1}{2}n$. Note that $n \geq 60$ and $p > \frac{5}{12}n$ imply that $p \geq 29$. Also, since $\frac{5}{12}n < p < \frac{1}{2}n$, it follows that $2p < n < 3p$, so an element of order p in S_n is either a p-cycle or the product of 2 disjoint p-cycles. Thus, the number of elements of order p in S_n is

$$C := \frac{n(n-1)(n-2)\cdots(n-p+1)}{p} + \frac{\frac{n(n-1)(n-2)\cdots(n-p+1)}{p} \cdot \frac{(n-p)(n-p-1)\cdots(n-2p+1)}{p}}{2}.$$

Then

$$\frac{n!}{C} = \frac{2p^2(n-p)!}{2p + (n-p)\cdots(n-2p+1)}.$$

Define

$$A := 2p^2(n-p)! \quad \text{and} \quad B := 2p + (n-p)\cdots(n-2p+1).$$

We show that B does not divide A. Let q be a prime divisor of B. We consider four ranges for q:

Case 1: $q \le p$. Since $B-2p$ is a product of $p \ge q$ consecutive integers, at least one of its factors is divisible by q. Thus, q divides $B-(B-2p) = 2p$, so that $q = 2$ or p.

Case 2: $p < q < n-2p+1$. Impossible, since $n < 3p$ implies $(n-2p+1)-p < 1$.

Case 3: $n-2p+1 \le q \le n-p$. Then q appears as a factor in $B-2p$. So again, $q = 2$ or p.

Case 4: $n-p < q$. Clearly q does not divide $A = 2p^2(n-p)!$. Thus, $B = 2^k p^m$. Observe that B is divisible by 2, but not by 4. Also, since $p < n-p < 2p$, we have that p^3 is the exact power of p that divides A. Hence, $k = 1$ and $m \le 3$. Therefore, $B \le 2p^3$. It follows that

$$\begin{aligned} 2p(p-1)(p+1) = 2p^3 - 2p \ge B - 2p &= (n-p)(n-p-1)\cdots(n-2p+1) \\ &> p(p-1)(p-2)(p-3)\cdots 3\cdot 2, \end{aligned}$$

since $n > 2p$. But this is impossible since $p \ge 29$.

Finally, to complete the proof, we need the number a_n of elements of order 2 in S_n, for $4 \le n \le 59$. By a result of Chowla, Herstein and Moore [Chowla et al. 1951], this number satisfies (for any n) the recurrence relation

$$a_n = a_{n-1} + (a_{n-2}+1)(n-1).$$

All that remains is to verify with a computer that $n!$ is never divisible by a_n for these values of n. □

3. The Proof of Theorem 1.11

In light of Theorems 1.2 and 1.3, it is enough to focus on groups all of whose Sylow subgroups are elementary abelian. Thus, throughout this section, we let

$$G \simeq (\mathbb{Z}_2)^t \times (\mathbb{Z}_{p_1})^{t_1} \times \cdots \times (\mathbb{Z}_{p_m})^{t_m},$$

where $p_1 < p_2 < \cdots < p_m$ are odd primes, and $m \ge 1$. Let

$$n = |G| = 2^t \prod_{i=1}^{m} p_i^{t_i} \quad \text{and} \quad f(n) = (2^t - 1)\prod_{i=1}^{m}(p_i^{t_i} - 1).$$

The following lemma is a direct consequence of the definition of a POS group.

Lemma 3.1. *The group G is a POS group if and only if $n/f(n)$ is an integer.*

Lemma 3.2. *If $m = 1$ and G is a POS group then $p_1 = 3$.*

Proof. Since $m = 1$, we have that $n = 2^t p_1^{t_1}$ and $f(n) = (2^t - 1)(p_1^{t_1} - 1)$. Then, since G is a POS group, $n/f(n)$ is an integer by Lemma 3.1. Thus, there exist positive integers a and b such that

$$a(2^t - 1) = p_1^{t_1} \qquad \text{and} \qquad b(p_1^{t_1} - 1) = 2^t. \tag{3-1}$$

Hence,

$$p_1^{t_1} - 2 \le 2^t - 1 \le p_1^{t_1}.$$

Thus, there are two cases to consider:

Case 1: $2^t - 1 = p_1^{t_1} - 2$. Then $p_1^{t_1} = 2^t + 1$, and so from (3-1) we conclude that $a = 1 + 2/(2^t - 1)$. Hence, $t = 1$, since a is an integer, which implies that $p_1 = 3$.

Case 2: $2^t - 1 = p_1^{t_1}$. We deduce from (3-1) that $p_1^{t_1} + 1 = 2^t$ and $p_1^{t_1} - 1 = 2^c$, for some $c < t$. Subtracting one equation from the other gives $2^c(2^{t-c} - 1) = 2$, which implies that $c = 1$ and $p_1 = 3$. □

Proof of Theorem 1.11. By way of contradiction, assume $p_1 > 3$. By Lemma 3.2, we may assume that $m \ge 2$. Let q be an arbitrary prime divisor of n. Since all prime divisors of $q - 1$ divide n, we have that $q \equiv 2 \pmod 3$ and all prime divisors of $q - 1$ are congruent to 2 modulo 3. Thus, we can recursively construct the list S of viable prime divisors of n as follows. Let $S_1 = [2, 5]$ and $q_1 = 5$. For $i \ge 2$, let q_i be the smallest prime such that $q_i > q_{i-1}$ and all prime divisors of $q_i - 1$ are contained in the list S_{i-1}. Define $S_i := [2, 5, \dots, q_{i-1}, q_i]$. Then

$$\begin{aligned}
S_2 &= [2, 5, 11], & q_2 &= 11,\\
S_3 &= [2, 5, 11, 17], & q_3 &= 17,\\
S_4 &= [2, 5, 11, 17, 23], & q_4 &= 23,\\
S_5 &= [2, 5, 11, 17, 23, 41], & q_5 &= 41,\\
S_6 &= [2, 5, 11, 17, 23, 41, 47], & q_6 &= 47,
\end{aligned}$$

and so on. Define $S := \lim_{i\to\infty} S_i$. Then

$$\frac{n}{f(n)} = \frac{2^t}{2^t - 1} \cdot \prod_{i=1}^{m} \frac{p_i^{t_i}}{p_i^{t_i} - 1} \le \frac{2^m}{2^m - 1} \cdot \prod_{i=1}^{m} \frac{p_i}{p_i - 1} \le \frac{2^m}{2^m - 1} \cdot \prod_{i=1}^{m} \frac{q_i}{q_i - 1}.$$

Using a computer, we have verified for $2 \le m \le 57096$ that

$$\frac{2^m}{2^m - 1} \prod_{i=1}^{m} \frac{q_i}{q_i - 1} < 2 \quad \text{and} \quad \frac{2^{57096}}{2^{57096} - 1} \prod_{i=1}^{57096} q_i > 4.48 \cdot 10^{457008}.$$

Clearly, $n/f(n) > 1$, and since $n/f(n)$ must be an integer by Lemma 3.1, the theorem follows. □

Remark 3.3. Whether or not the list S constructed in the proof of Theorem 1.11 is finite, sieve methods [Halberstam and Richert 1974] can be used to show that the product

$$\frac{2^m}{2^m-1}\prod_{i=1}^{m}\frac{q_i}{q_i-1} \tag{3-2}$$

is bounded above. We conjecture that (3-2) is less than 2 for all $m \geq 2$, but we are unable to provide a proof since a tight explicit bound is both tedious and difficult to compute using sieve methods. The truth of this conjecture would imply that the answer to Question 1.9 is affirmative.

4. The proof of Theorem 1.12

Definition 4.1. Let t be a positive integer, and let q be a prime divisor of 2^t-1. We say that q is a *primitive divisor* of 2^t-1 if q does not divide 2^s-1 for any positive integer $s<t$.

Theorem 4.2 [Bang 1886]. *Let $t \geq 2$ be an integer. Then 2^t-1 has a primitive divisor except when $t=6$.*

Theorem 4.3. *Let G be a minimal abelian POS group, such that*

$$G \simeq (\mathbb{Z}_2)^t \times \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_{k-1}} \times (\mathbb{Z}_{p_k})^2 \times \mathbb{Z}_{p_{k+1}} \times \cdots \times \mathbb{Z}_{p_m},$$

where $p_1 < p_2 < \cdots < p_m$ are odd primes. Then $p_1 = 3$ and $2^t - 1 = 2^{p_k} - 1 = p_i p_j$, for some $i \neq j$.

Proof. As before, let

$$n = |G| = 2^t p_k^2 \prod_{\substack{i=1\\ i\neq k}}^{m} p_i \quad \text{and} \quad f(n) = (2^t-1)(p_k^2-1)\prod_{\substack{i=1\\ i\neq k}}^{m}(p_i-1).$$

Since G is a POS group, $n/f(n)$ is an integer by Lemma 3.1.

Next, note that $n \equiv 0 \pmod 3$. For if not, then $p_k > 3$ and $p_k^2 - 1 \equiv 0 \pmod 3$. Then, since $f(n) \equiv 0 \pmod{p_k^2-1}$, we have that $f(n) \equiv 0 \pmod 3$, which contradicts the fact that $n/f(n)$ is an integer. This proves that $p_1 = 3$.

Now, suppose that p is an odd prime divisor of t. Then 2^p-1 divides 2^t-1, and so 2^p-1 divides n. Consequently, every prime divisor of 2^p-1 is p_i for some i, and then $p_i - 1 \equiv 0 \pmod p$. Also, for each such p_i, we have that $p_i - 1$ divides n. Thus, since n is not divisible by the cube of any odd prime, it follows that 2^p-1 has at most two distinct odd prime divisors. Therefore, we are led to consider the following five cases:

(1) $2^p - 1 = p_k^2$ for some odd prime divisor p of t.

(2) $2^p - 1 = p_i p_k^2$ for some i, and some odd prime divisor p of t.

(3) There exists an odd prime that divides t, and for every odd prime p that divides t, we have that $2^p - 1 = p_i$ for some i.

(4) There exists at least one odd prime p that divides t such that $2^p - 1 = p_i p_j$ for some $i \neq j$.

(5) No odd prime divides t; that is $t = 2^a$.

Ljunggren [1943] proved that Case (1) is impossible.

In Case (2), we have that $p_i - 1 \equiv 0 \pmod{p}$ and $p_k - 1 \equiv 0 \pmod{p}$. Then $(p_i - 1)(p_k^2 - 1) \equiv 0 \pmod{p^2}$, which says that p^2 divides n. Hence, $p = p_k$. But this contradicts the fact that $p_k - 1 \equiv 0 \pmod{p}$. Hence, Case (2) is impossible as well.

For Case (3), we show first that t has exactly one odd prime divisor. Suppose that p and q are odd prime divisors of t. Then $2^p - 1 = p_i$ and $2^q - 1 = p_j$ for some i and j. Then $p_i - 1 \equiv 0 \pmod{p}$ and $p_j - 1 \equiv 0 \pmod{q}$. By Theorem 4.2, there exists an odd prime $r \neq p_i, p_j$ such that $2^{pq} - 1 \equiv 0 \pmod{r}$. Since $2^{pq} - 1$ divides $2^t - 1$, we have that $f(n) \equiv 0 \pmod{r}$, and so $r = p_v$ for some v. Since p_v is a primitive divisor, it follows that $p_v - 1 \equiv 0 \pmod{pq}$. But then $(p_i - 1)(p_v - 1) \equiv 0 \pmod{p^2}$, and $(p_j - 1)(p_v - 1) \equiv 0 \pmod{q^2}$, which implies that $p = q$.

Thus, t has at most one odd prime divisor. Suppose $t = 2^a p^b$. Let $2^p - 1 = p_i$. Then $p_i - 1 \equiv 0 \pmod{p}$. If $b \geq 2$, we can use Theorem 4.2 to produce a prime divisor $p_j \neq p_i$ of $2^{p^2} - 1$ such that $p_j - 1 \equiv 0 \pmod{p^2}$. But then $(p_i - 1)(p_j - 1) \equiv 0 \pmod{p^3}$, which contradicts the fact that $n/2^t$ is cube-free. Therefore, we only need to consider here the two possibilities $t = 2^a p$ and $t = p$, since the possibility that $t = 2^a$ is handled separately below as Case (5).

Suppose first that $t = 2^a p$. As before, let $2^p - 1 = p_i$. Then $p_i - 1 \equiv 0 \pmod{3}$ and $p_i - 1 \equiv 0 \pmod{p}$. Suppose that $a \geq 1$. Then $2^t - 1 \equiv 0 \pmod{3}$, so that $(2^t - 1)(p_i - 1) \equiv 0 \pmod{9}$, which implies that $p_k = 3$. If $p = 3$, then $2^6 - 1$ divides $2^t - 1$, and so $(2^t - 1)(p_i - 1) \equiv 0 \pmod{27}$, which is a contradiction. On the other hand, if $p \neq 3$, then by Theorem 4.2, there exists a prime $q \neq p_i$ such that $q - 1 \equiv 0 \pmod{2^a p}$. Hence, $(p_i - 1)(q - 1) \equiv 0 \pmod{p^2}$, which implies that $p = p_k = 3$, again a contradiction. Therefore, $a = 0$ and $t = p$, which is the second possibility above. Again, let $2^p - 1 = p_i$. Then $p_i - 1 \equiv 0 \pmod{p}$, so that $p \neq p_i$. Also, $p_i - 1 \equiv 0 \pmod{3}$. If $p_k \neq 3$, then $(p_k^2 - 1)(p_i - 1) \equiv 0 \pmod{9}$, which is impossible since the only square that divides n is $p_k^2 \neq 9$. Hence, $p_k = 3$. If $p = 3 = p_k$, then $n \equiv 0 \pmod{8}$, but $n \not\equiv 0 \pmod{16}$. However, if $p = 3$, then n would be divisible by $(2^{p_k} - 1)(p_k^2 - 1) = (7 - 1)(3^2 - 1)$, which implies that $n \equiv 0 \pmod{16}$. This contradiction shows that $p \neq 3$. Also, since p is odd, we have that $p_i \neq 3$. Thus, all three primes p, p_i and $p_k = 3$ are distinct. If $p \equiv 1 \pmod{3}$, then $2^6 - 1$ divides $2^{p-1} - 1 = p_i - 1$, and so the number of elements of order pp_i is

$$(p-1)(p_i-1) = 2(p-1)(2^{p-1}-1) \equiv 0 \pmod{27},$$

which does not divide n. Thus, $p \equiv 2 \pmod 3$. Now, let q be an odd prime divisor of $p-1$. Then 2^q-1 and $2^{2q}-1$ divide $2^{p-1}-1$, and so both divide n. Let r be a primitive divisor of 2^q-1, and let s be a primitive divisor of $2^{2q}-1$. Since $p \equiv 2 \pmod 3$, we have that $q \neq 3$, and therefore the existence of s is guaranteed by Theorem 4.2. Then

$$r-1 \equiv 0 \equiv s-1 \pmod q.$$

Since $r \neq s$, it follows that either $r \neq p$ or $s \neq p$. Suppose, without loss of generality, that $r \neq p$. Note that $r \neq 3$ so that the number of elements of order pr is $(p-1)(r-1)$. But

$$(p-1)(r-1) \equiv 0 \pmod{q^2},$$

which implies that $q = 3$, a contradiction. Hence, we conclude that no odd primes divide $p-1$. Write $p-1 = 2^a$. Then the number of elements of order p_i is

$$p_i - 1 = 2^p - 2 = 2(2^{2^a}-1) \equiv 0 \pmod 3.$$

If $a \geq 7$, then 6700417 and 274177 divide $2^{2^a}-1$, and the number of elements of order $p_i \cdot 6700417 \cdot 274177$ is

$$2(2^{2^a}-1)(6700416)(274176) \equiv 0 \pmod{27},$$

which does not divide n. Hence, $a \leq 6$, and it is easy to check that 2^a+1 is prime exactly when $a = 1$, 2 or 4. Since $p \equiv 2 \pmod 3$, then $a = 2$ or 4. If $a = 2$, then $p = 5$, and $31 = 2^5-1$ divides n. But then, the number of elements of order $3^2\cdot 5\cdot 31$, which is $(3^2-1)(5-1)(31-1) = 2^6\cdot 3\cdot 5$, does not divide n. Similarly, if $a = 4$, then $p = 17$, and the power of 2 that divides $f(n)$ is greater than the power of 2 that divides n. Therefore, Case (3) is impossible.

We proceed now to Case (4). Suppose that p is an odd prime dividing t such that $2^p-1 = p_i p_j$, for some $i \neq j$. Then $p_i - 1 \equiv p_j - 1 \equiv 0 \pmod p$, so that p^2 divides the number of elements of order $p_i p_j$, and thus p^2 divides n. Hence, $p = p_k$. If there exists a prime $q \neq p$ that divides t, then $2^{pq}-1$ divides n. By Theorem 4.2, there is a primitive divisor p_s of $2^{pq}-1$ with $s \notin \{i, j\}$. Then p divides $p_s - 1$, and hence p^3 divides $(p_i-1)(p_j-1)(p_s-1)$, the number of elements of order $p_i p_j p_s$. This contradiction shows that $p = p_k$ is the only odd prime that divides t. An argument similar to the one used in Case (3) shows that p^2 does not divide t. Then, as in Case (3), we only have to consider the two possibilities: $t = 2^a p$ and $t = p$. Suppose that $t = 2^a p$, with $a \geq 1$. Since $2^p - 1 = p_i p_j$, with $i \neq j$, it follows that $p \neq 3$. Then, by Theorem 4.2, there exists a primitive divisor p_s

of $2^{2p}-1$. Thus, $s \notin \{i, j\}$ and $p_s - 1 \equiv 0 \pmod{p}$. But then we have that the number of elements in G of order $p_i p_j p_s$ is

$$(p_i-1)(p_j-1)(p_s-1) \equiv 0 \pmod{p^3}.$$

Hence, $a = 0$ and $t = p = p_k$.

This brings us to Case (5). Assume now that $t = 2^a$. As in Case (3), if $a \geq 7$, then 6700417 and 274177 divide $2^{2^a}-1$, and n is divisible by the number of elements in G of order $2 \cdot 6700417 \cdot 274177$, which is $(2^{2^a}-1)(6700416)(274176)$. But $(2^{2^a}-1)(6700416)(274176)$ cannot divide n since

$$(2^{2^a}-1)(6700416)(274176) \equiv 0 \pmod{27},$$

and $n/2^t$ is cube-free. Thus, $a \leq 6$. It is straightforward to check that each of these cases, in some way, violates the hypotheses of the theorem. For example, if $a = 6$, then n is divisible by

$$2^{64}-1 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 641 \cdot 65537 \cdot 6700417.$$

Hence, $(2^{64}-1) \cdot 640$ and $(2^{64}-1) \cdot 6700416$ must also divide n. However, $(2^{64}-1) \cdot 640 \equiv 0 \pmod{25}$ and $(2^{64}-1) \cdot 6700416 \equiv 0 \pmod{9}$, which contradicts the fact that n is divisible by exactly one odd square. Checking the remaining cases completes the proof of the theorem. □

Remark 4.4. Without loss of generality, we can assume that $p_i < p_j$ in the statement of the conclusion of Theorem 4.3. Also, this conclusion implies that $3 = p_1 < p_k < p_i < p_j$, with $p_k \geq 11$. Thus, $m \geq 4$.

Proof of Theorem 1.12. Let G be a minimal abelian POS group such that

$$G \simeq (\mathbb{Z}_2)^t \times \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_{k-1}} \times (\mathbb{Z}_{p_k})^2 \times \mathbb{Z}_{p_{k+1}} \times \cdots \times \mathbb{Z}_{p_m},$$

where $p_1 < p_2 < \cdots < p_m$ are odd primes, with $1 \leq m \leq 5$. By Theorem 4.3, we have that $p_1 = 3$ and $2^t - 1 = 2^{p_k} - 1 = p_i p_j$ for some $i \neq j$. By Remark 4.4, we can also assume that $p_k \geq 11$ and that $m = 4$ or $m = 5$.

Consider first the case when $m = 4$. In this case, we have

$$\frac{n}{f(n)} = \frac{2^{p_k} \cdot 3 \cdot p_k^2 \cdot p_i \cdot p_j}{(2^{p_k}-1) \cdot 2 \cdot (p_k^2-1) \cdot (p_i-1) \cdot (p_j-1)} = \frac{2^{p_k-1} \cdot 3 \cdot p_k^2}{(p_k^2-1) \cdot (p_i-1) \cdot (p_j-1)}.$$

Since $p_i - 1 \equiv p_j - 1 \equiv 0 \pmod{p_k}$, it follows that either

(1) $p_k - 1 = 2^a \cdot 3$ and $p_k + 1 = 2^b$ or

(2) $p_k - 1 = 2^a$ and $p_k + 1 = 2^b \cdot 3$.

In (1), we get that

$$2 = 2^b - 2^a \cdot 3 = 2^a(2^{b-a} - 3),$$

which implies that $a = 1$ and $b = 3$. Hence, $p_k = 7$, which contradicts the fact that $p_k \geq 11$. In (2), we get two possibilities. The first possibility gives

$$2 = 2^a(2^{b-a} \cdot 3 - 1),$$

which implies that $a = b = 0$. Thus $p_k = 2$, which is impossible. The second possibility yields

$$2 = 2^b(3 - 2^{a-b}),$$

which implies that either $a = 2$ and $b = 1$, in which case $p_k = 5$; or $a = b = 0$, in which case $p_k = 2$. Both situations are impossible. Hence, there are no POS groups satisfying the conditions of the theorem with $m = 4$.

Now suppose that $m = 5$. Then

$$\frac{n}{f(n)} = \frac{2^{p_k} \cdot 3 \cdot p \cdot p_k^2 \cdot p_i \cdot p_j}{(2^{p_k} - 1) \cdot 2 \cdot (p-1) \cdot (p_k^2 - 1) \cdot (p_i - 1) \cdot (p_j - 1)}.$$

Since $p_k < p_i < p_j$, we have $\frac{p_j}{p_j - 1} < \frac{p_i}{p_i - 1} < \frac{p_k}{p_k - 1}$. Thus,

$$\frac{n}{f(n)} \leq \frac{2^{p_k} \cdot 3 \cdot 5 \cdot p_k^4}{(2^{p_k} - 1) \cdot 2 \cdot 4 \cdot (p_k^2 - 1) \cdot (p_k - 1)^2}.$$

It is straightforward to show that

$$g(x) = \frac{15 \cdot 2^x \cdot x^4}{8 \cdot (2^x - 1)(x^2 - 1)(x - 1)^2}$$

is a decreasing function for $x \geq 2$, and that $g(x) < 2$ when $x \geq 32$. It follows that $n/f(n) < 2$ when $p_k \geq 37$. Clearly, $n/f(n) > 1$, and since we are assuming that $n/f(n)$ is an integer, we only have to check p_k with $11 \leq p_k \leq 31$. The fact that $2^{p_k} - 1$ must be the product of two distinct primes rules out all primes in this range except $p_k = 11$ and $p_k = 23$. If $p_k = 23$, then $2^{23} - 1 = 47 \cdot 178481$ divides n. But then $178481 - 1 = 2^4 \cdot 5 \cdot 23 \cdot 97$ also divides n, which contradicts the fact that $m = 5$. Verifying that the case $p_k = 11$ gives the POS group in the statement of the theorem completes the proof. □

Acknowledgments

The authors thank the referee for the many valuable suggestions.

References

[Bang 1886] A. S. Bang, "Taltheoretiske undersøgelser", *Tidsskr. Math.* (5) **4** (1886), 70–80, 130–137. Zbl 19.0168.02

[Chebyshev 1852] P. L. Chebyshev, "Mémoire sur les nombres premiers", *J. Math. Pures Appl.* (1) **17** (1852), 366–390.

[Chowla et al. 1951] S. Chowla, I. N. Herstein, and W. K. Moore, "On recursions connected with symmetric groups, I", *Canadian J. Math.* **3** (1951), 328–334. MR 13,10c Zbl 0043.25904

[Das 2009] A. K. Das, "On finite groups having perfect order subsets", *Int. J. Algebra* **3**:13 (2009), 629–637. MR 2010j:20035 Zbl 1197.20018

[Finch and Jones 2002] C. E. Finch and L. Jones, "A curious connection between Fermat numbers and finite groups", *Amer. Math. Monthly* **109**:6 (2002), 517–524. MR 2003d:11016 Zbl 1058.11009

[Finch and Jones 2003] C. E. Finch and L. Jones, "Nonabelian groups with perfect order subsets", *JP J. Algebra Number Theory Appl.* **3**:1 (2003), 13–26. Corrigendum in **4**:2 (2004), 413–416. MR 2004d:20023 Zbl 1052.20016

[Halberstam and Richert 1974] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs **4**, Academic Press, London, 1974. MR 54 #12689 Zbl 0298.10026

[Libera and Tlucek 2003] S. Libera and P. Tlucek, "Some perfect order subset groups", *Pi Mu Epsilon J.* **11**:9 (2003), 495–498.

[Ljunggren 1943] W. Ljunggren, "Noen setninger om ubestemte likninger av formen $\frac{x^n-1}{x-1}=y^q$", *Norsk Mat. Tidsskr.* **25** (1943), 17–20. MR 8,315a Zbl 0028.00901

[Nagura 1952] J. Nagura, "On the interval containing at least one prime number", *Proc. Japan Acad.* **28**:4 (1952), 177–181. MR 14,355b Zbl 0047.04405

[Tuan and Hai 2010] N. T. Tuan and B. X. Hai, "On perfect order subsets in finite groups", *Int. J. Algebra* **4**:21 (2010), 1021–1029. MR 2012b:20057 Zbl 1219.20023

Received: 2010-07-23 Accepted: 2011-06-15

lkjone@ship.edu *Department of Mathematics, Shippensburg University, 1871 Old Main Drive, Shippensburg, PA 17257, United States*

kt5638@ship.edu *Department of Mathematics, Shippensburg University, Shippensburg, PA 17257, United States*

involve

msp.berkeley.edu/involve

See inside back cover or http://msp.berkeley.edu/involve for submission instructions.

The subscription price for 2011 is US $100/year for the electronic version, and $130/year (+$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

involve

2011 vol. 4 no. 3

1944-4176(2011)4:3;1-C