

# Order Dimension of Subgroups

Iordan Ganev

## 1 Introduction

Abstract Algebra textbooks sometimes pose versions of the following exercise: In a group  $G$  of order 65, let  $a$  and  $b$  be nonidentity elements of different orders and prove that no proper subgroup of  $G$  contains  $a$  and  $b$ . A solution is: Suppose  $H$  is a subgroup of  $G$  that contains  $a$  and  $b$ . If either  $a$  or  $b$  has order 65, then  $H = G$ . Otherwise, if the two elements have orders 5 and 13, then 5 and 13 must divide the order of the  $H$  (by Lagrange). The least common multiple of 5 and 13 is 65 and  $H \subseteq G$ , so  $|H| = 65$  and  $H = G$ . Thus, no proper subgroup of  $G$  contains  $a$  and  $b$ . More generally, if  $|G| = pq$ , where  $p$  and  $q$  are distinct primes, then the same argument shows that the only subgroup that contains two nonidentity elements of different orders is  $G$  itself.

Now let  $r$  be another prime and let  $|G| = pqr$ . In this case, it is possible that  $G$  has a proper subgroup of order  $pq$  that contains three nonidentity elements of orders  $p$ ,  $q$ , and  $pq$ . Can a proper subgroup  $H$  contain four nonidentity elements of different orders? No, because a proper subgroup  $H$  must have order  $p$ ,  $q$ ,  $r$ ,  $pq$ ,  $pr$ , or  $qr$ . Each of these cases allows for less than four nonidentity elements of different orders in  $H$ . Hence, three is the “bound” for the number of nonidentity elements of different orders that can be contained in a proper subgroup of  $G$ .

## 2 Order Dimension for Groups and Subgroups

A natural generalization of these observations is to determine the maximum number of nonidentity elements of different orders that can be contained in a subgroup of a group of any order. We define

$\text{odim}(G)$ , the *order dimension* of the group  $G$ , as the number of different orders of its nonidentity elements. For example, the  $\text{odim}(D_3) = 2$  since nonidentity elements are either rotations with order 3, or reflections with order 2. In  $\mathbb{Z}_{12}$ , there are nonidentity elements with orders 2, 3, 4, 6, and 12, so  $\text{odim}(\mathbb{Z}_{12}) = 5$ .

Let  $G$  be a group with order  $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ . It is well-known from number theory that the number of divisors of  $n$  is  $(n_1 + 1)(n_2 + 1) \dots (n_k + 1)$ . This is because each divisor has the form  $p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$ , where each  $l_i$  can take on the  $n_i + 1$  possible values  $0, 1, \dots, n_i$ . Since the order of each nonidentity element is a divisor other than 1, the order dimension of  $G$  cannot exceed the number of divisors of  $n$  minus one; that is,  $\text{odim}(G) \leq (n_1 + 1)(n_2 + 1) \dots (n_k + 1) - 1$ . For a group  $G$  of order  $65 = 5 \cdot 13$ ,  $\text{odim}(G) \leq (1 + 1)(1 + 1) - 1 = 3$ . Indeed, nonidentity elements may have order 5, 13, or 65. Similarly, when  $|G| = pq$ ,  $\text{odim}(G) \leq 3$ , and when  $|G| = pqr$ ,  $\text{odim}(G) \leq (1 + 1)(1 + 1)(1 + 1) - 1 = 7$ .

We seek to establish a more specific maximum for the order dimension of any proper subgroup of  $G$ . For example, if  $|G| = 65$  or any integer of the form  $pq$  [a product of two distinct primes], we know from above that although  $\text{odim}(G) \leq 3$ , the order dimension of any proper subgroup is less than or equal to 1. Also, if  $|G| = pqr$  and  $H$  is a proper subgroup, then  $\text{odim}(H) \leq 3$ , more specific than the maximum of 7 for  $\text{odim}(G)$ . In order generalize, we renumber the prime factors of  $|G| = n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$  so that  $n_1$  is the greatest of all the powers [ $n_1 \geq n_i$  for  $i = 2, 3, \dots, k$ ], and we define  $b_n = n_1(n_2 + 1) \dots (n_k + 1) - 1$ .

Theorem 1. If  $G$  is a group of order  $n$  and  $H$  is a proper subgroup of  $G$ , then  $\text{odim}(H) \leq b_n$ .

Proof. Since the order of  $H$  divides the order of  $G$  and  $H$  is proper,  $|H|$  has the form  $p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$  where  $0 \leq l_i \leq n_i$  for  $i = 1, 2, \dots, k$  and  $l_i < n_i$  for some  $i$ . The number of divisors of  $|H|$ , excluding the divisor one, is an upper bound to the order dimension of  $H$ , so  $\text{odim}(H) \leq (l_1 + 1)(l_2 + 1) \dots (l_k + 1) - 1$ .

In the case that  $l_1 < n_1$ , we note that  $l_1 + 1 \leq n_1$ . Then,

$$\begin{aligned} \text{odim}(H) &\leq (l_1 + 1)(l_2 + 1) \dots (l_k + 1) - 1 \\ &\leq (l_1 + 1)(n_2 + 1) \dots (n_k + 1) - 1 \\ &\leq n_1(n_2 + 1) \dots (n_k + 1) - 1 = b_n. \end{aligned}$$

Now we may assume that  $l_1 = n_1$ . Since  $H$  is proper,  $l_i < n_i$  and  $l_i + 1 \leq n_i$  for some  $i \neq 1$  and  $\text{odim}(H) \leq (l_1 + 1)(l_2 + 1) \dots (l_i + 1) \dots (l_k + 1) - 1 \leq (n_1 + 1)(n_2 + 1) \dots (l_i + 1) \dots (n_k + 1) - 1$ . Suppose this

quantity exceeds  $b_n$ :

$$b_n < (n_1 + 1)(n_2 + 1)\dots(l_i + 1)\dots(n_k + 1) - 1.$$

Then,

$$n_1(n_2 + 1)\dots(n_i + 1)\dots(n_k + 1) - 1 < (n_1 + 1)(n_2 + 1)\dots(l_i + 1)\dots(n_k + 1) - 1$$

$$\Rightarrow n_1(n_i + 1) < (n_1 + 1)(l_i + 1) \leq (n_1 + 1)n_i$$

$$\Rightarrow n_1n_i + n_1 < n_1n_i + n_i$$

$$\Rightarrow n_1 < n_i \text{ — a contradiction.}$$

Thus,  $b_n \geq (n_1 + 1)(n_2 + 1)\dots(l_i + 1)\dots(n_k + 1) - 1 \geq (l_1 + 1)(l_2 + 1)\dots(l_i + 1)\dots(l_k + 1) - 1 \geq \text{odim}(H)$ .  $\diamond$

A group  $G$  may (or may not) have a subgroup  $H$  with  $\text{odim}(H) = b_n$  where  $n$  is the order  $G$ . In such cases, we say that the group  $G$  has *property #*.

Example 1.  $\mathbb{Z}_n$  always has property # because cyclic groups have an element of every possible order. For instance, take  $\mathbb{Z}_{56}$ . Since  $56 = 2^3 \cdot 7$  and  $n_1 = 3$ , we have  $b_{56} = 3(1 + 1) - 1 = 5$ . Indeed,  $\text{odim}(\langle 2 \rangle) = 5$  since  $\langle 2 \rangle$  contains the elements 2, 4, 8, 14, and 28, which have orders 28, 14, 7, 4, and 2, respectively. In general, if  $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ , where  $n_1$  is the greatest power, then  $\text{odim}(\langle p_1 \rangle) = b_n$ .

Example 2. The maximal power ( $n_1$ ) in the prime-power expansion of  $|G| = n$  may not be unique to a single prime, and there may be subgroups of different orders whose order dimension is  $b_n$ . In  $\mathbb{Z}_{216}$ , for instance, the order of the group is  $216 = 2^3 \cdot 3^3$ . The subgroups  $\langle 2 \rangle$  and  $\langle 3 \rangle$  have different orders, but  $\text{odim}(\langle 2 \rangle) = \text{odim}(\langle 3 \rangle) = b_{216} = 3(3 + 1) - 1 = 11$ .

Example 3. The alternating group  $A_4$  of order  $12 = 2^2 \cdot 3$  does not have property #. In this case, property # would require there to be a proper subgroup with order dimension equal to  $b_{12} = 2(1 + 1) - 1 = 3$ . This can only occur if the subgroup has order 6, since groups of orders 2, 3, or 4 have order dimension less than 3.  $A_4$  has no subgroup of order 6, hence it does not have property #.

Example 4. The group  $\mathbb{Z}_3 \oplus \mathbb{Z}_{90}$  has order  $270 = 3^3 \cdot 2 \cdot 5$  and  $b_{270} = 3(1 + 1)(1 + 1) - 1 = 11$ . Now,  $\langle (0, 1) \rangle$  is isomorphic to  $\mathbb{Z}_{90}$ , which has order dimension  $(2 + 1)(1 + 1)(1 + 1) - 1 = 11$  since  $90 = 3^2 \cdot 2 \cdot 5$ . But this is precisely  $b_{270}$ , so  $\mathbb{Z}_3 \oplus \mathbb{Z}_{90}$  has property #. Also, the elements  $(1, 1)$  and  $(2, 1)$  have order 90, so  $\langle (1, 1) \rangle$  and  $\langle (2, 1) \rangle$  are subgroups isomorphic to  $\mathbb{Z}_{90}$ . We can conclude that  $\text{odim}(\langle (0, 1) \rangle) = \text{odim}(\langle (1, 1) \rangle) = \text{odim}(\langle (2, 1) \rangle) = b_{270}$ .

Example 5. Consider  $D_8$ , the group of symmetries of a regular octagon. Here,  $|D_8| = 16 = 2^4$  and  $b_{16} = 4 - 1 = 3$ .  $D_8$  has property  $\#$  and a subgroup whose order dimension is  $b_{16}$  is  $\langle R_{45} \rangle$ . Indeed,  $R_{45}$ ,  $R_{135}$ ,  $R_{225}$ , and  $R_{315}$  are elements of  $\langle R_{45} \rangle$  with order 8;  $R_{90}$ , and  $R_{270}$  have order 4;  $R_{180}$  has order 2; and  $R_0$  is the identity.

Example 6. The group of symmetries of a regular nonagon,  $D_9$ , has order  $18 = 3^2 \cdot 2$  and  $b_{18} = 2(2 + 1) - 1 = 5$ . Reflections in  $D_9$  all have order 2 and rotations have order 3 or 9, hence the order dimension of  $D_9$  is 3. It is impossible for a proper subgroup of  $D_9$  to have higher order dimension than the group itself, so  $D_9$  does not have property  $\#$ .

Continue to assume  $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ , where  $p_1$  is the prime or one of the primes with the highest power; that is,  $n_1 \geq n_i$  for  $i = 1, 2, \dots, k$ . The examples suggest the following theorem.

Theorem 2. Let  $G$  be a group of order  $n$ , and let  $H$  be a proper subgroup of  $G$ . Then  $\text{odim}(H) = b_n$  if and only if  $H \approx \mathbb{Z}_{n/p_1}$ .

Proof. Suppose  $\text{odim}(H) = b_n$ . Since  $H$  is a proper subgroup of  $G$ ,  $|H|$  has the form  $p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$  where  $0 \leq l_i \leq n_i$  for  $i = 1, 2, \dots, k$  and  $l_i < n_i$  for some  $i$ .

If  $l_1 < n_1$ , then the proof of Theorem 1 shows that

$$\text{odim}(H) \leq (l_1 + 1)(l_2 + 1) \dots (l_k + 1) - 1 \leq (l_1 + 1)(n_2 + 1) \dots (n_k + 1) - 1 \leq n_1(n_2 + 1) \dots (n_k + 1) - 1 = b_n.$$

Since  $\text{odim}(H) = b_n$ , the inequalities become equalities. Therefore,  $l_1 + 1 = n_1$ ,  $l_i = n_i$  for  $i = 2, 3, \dots, k$ ,

and  $|H| = p_1^{n_1-1} p_2^{n_2} \dots p_k^{n_k} = \frac{n}{p_1}$ . This subgroup must have an element with order corresponding to every

divisor of  $|H| = p_1^{n_1-1} p_2^{n_2} \dots p_k^{n_k}$ , and in particular  $H$  contains an element with order  $p_1^{n_1-1} p_2^{n_2} \dots p_k^{n_k} = |H|$ .

That element generates the whole subgroup, so  $H$  is cyclic. Every cyclic group of order  $\frac{n}{p_1}$  is isomorphic to  $\mathbb{Z}_{n/p_1}$ , so  $H \approx \mathbb{Z}_{n/p_1}$ .

Otherwise,  $l_1 = n_1$ . Since  $H$  is proper, we know  $l_i < n_i$  for some  $i$  with  $2 \leq i \leq k$ . The proof of Theorem 1 demonstrates that

$$b_n \geq (n_1 + 1)(n_2 + 1) \dots (l_i + 1) \dots (n_k + 1) - 1 \geq (l_1 + 1)(l_2 + 1) \dots (l_i + 1) \dots (l_k + 1) - 1 \geq \text{odim}(H).$$

Now,  $\text{odim}(H) = b_n$  implies

$$b_n = (n_1 + 1)(n_2 + 1) \dots (l_i + 1) \dots (n_k + 1) - 1 = (l_1 + 1)(l_2 + 1) \dots (l_i + 1) \dots (l_k + 1) - 1 = \text{odim}(H),$$

so  $l_j = n_j$  for all  $j$  from 1 to  $k$  except  $i$ . To find  $l_i$ , we substitute the definition of  $b_n$  and reduce:

$$\begin{aligned}
n_1(n_2 + 1)\dots(n_i + 1)\dots(n_k + 1) - 1 &= (n_1 + 1)(n_2 + 1)\dots(l_i + 1)\dots(n_k + 1) - 1 \\
&\Rightarrow n_1(n_i + 1) = (n_1 + 1)(l_i + 1) \\
&\Rightarrow n_1n_i + n_1 = n_1l_i + l_i + n_1 + 1 \\
&\Rightarrow n_1n_i = n_1l_i + l_i + 1 \\
&\Rightarrow n_1(n_i - l_i) = l_i + 1.
\end{aligned}$$

Now,  $n_1 \leq n_1(n_i - l_i) = l_i + 1 \leq n_i \leq n_1$ , so we get  $n_i = n_1$ . This means  $p_i$  could have been chosen as the prime with the greatest power instead of  $p_1$ . We refer to the first case of this proof to see that

$$H \approx \mathbb{Z}_{n/p_i}.$$

For the converse, suppose  $\mathbb{Z}_{n/p_1} \approx H$ . Then  $|H| = p_1^{n_1-1}p_2^{n_2}\dots p_k^{n_k}$  and, as a cyclic group,  $H$  has at least one element for every divisor of  $|H|$ . Therefore,

$$\text{odim}(H) = n_1(n_2 + 1)\dots(n_k + 1) - 1 = b_n. \diamond$$

Corollary. A group  $G$  of order  $n$  has property  $\#$  if and only if it has a subgroup isomorphic to  $\mathbb{Z}_{n/p_1}$ .

### 3 Finitely Generated Abelian Groups

Example 7. The group  $\mathbb{Z}_2 \oplus \mathbb{Z}_{54}$  has order  $108 = 3^3 \cdot 2^2$ , so property  $\#$  would require cyclic subgroup isomorphic to  $\mathbb{Z}_{108/3} = \mathbb{Z}_{36}$ , or, equivalently, an element of order 36. Elements in  $\mathbb{Z}_2$  have order 1 or 2, while elements in  $\mathbb{Z}_{54}$  have order 1, 2, 3, 6, 9, 18, or 54. The order of an element  $(x, y) \in \mathbb{Z}_2 \oplus \mathbb{Z}_{54}$  is the least common multiple of  $|x|$  and  $|y|$ , hence  $|(x, y)| = 1, 2, 3, 6, 9, 18, \text{ or } 54$ . Since 36 does not appear on this list,  $\mathbb{Z}_2 \oplus \mathbb{Z}_{54}$  does not have property  $\#$ .

We established in Example 4 that  $\mathbb{Z}_3 \oplus \mathbb{Z}_{90}$  has property  $\#$ , but Example 7 shows that not all external direct products of finite cyclic groups — that is, not all finitely generated abelian groups — have property  $\#$ . Theorem 3 explores these groups further and continues to assume  $n = p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$ , where  $p_1$  is the prime or one of the primes with the highest power; that is,  $n_i \geq n_1$  for  $i = 1, 2, \dots, k$ .

Theorem 3. Let  $G$  be a finitely generated abelian group of order  $n$ .  $G$  has property  $\#$  if and only if  $G$  is isomorphic to  $\mathbb{Z}_n$  or  $\mathbb{Z}_{p_1} \oplus \mathbb{Z}_{n/p_1}$

Proof. Suppose  $G$  has property  $\#$ . The corollary to Theorem 2 asserts that there must be an element of order  $n/p_1$ . By the Fundamental Theorem of Finitely-Generated Abelian Groups,  $G$  is isomorphic to  $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{m_r}$ , where  $m_1$  divides  $m_2$ ,  $m_2$  divides  $m_3$ , and so on. We examine  $\mathbb{Z}_{m_r} = \mathbb{Z}_{n/d}$  for some divisor  $d$  of  $n$ . Let  $(x_1, x_2, \dots, x_r)$  be the element of order  $n/p_1$ . Now,  $|x_1|$  divides  $m_1$ ,  $|x_2|$  divides  $m_2$ , ..., and  $|x_r|$  divides  $m_r$  (by Lagrange). Since all the  $m$ 's divide  $m_r$ ,  $|x_i|$  divides  $m_1$  for all  $i = 1, 2, \dots, r$ . Consequently,

$$\begin{aligned} \frac{n}{p_1} &= \text{lcm}(|x_1|, |x_2|, \dots, |x_r|) \text{ divides } m_r = \frac{n}{d} \\ &\Rightarrow \left(\frac{n}{p_1}\right)q = \frac{n}{d} \\ &\Rightarrow p_1 = dq \\ &\Rightarrow d = 1, q = p_1; \text{ or } d = p_1, q = 1 \\ &\Rightarrow G \approx \mathbb{Z}_n \text{ or } G \approx \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{n/p_1}. \end{aligned}$$

For the converse, suppose  $G \approx \mathbb{Z}_n$  or  $G \approx \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{n/p_1}$ . Then examples of cyclic groups of order  $n/p_1$  are  $\langle p_1 \rangle$  in the first case and  $\langle (0, 1) \rangle$  in the second, so in both cases  $G$  has property  $\#$ .  $\diamond$

## 4 Dihedral Groups

Recall from Examples 5 and 6 that  $D_8$  has property  $\#$  and  $D_9$  does not. Why do dihedral groups have property  $\#$  and others do not? The general result is given in the next theorem.

Theorem 4. Let  $n = 2m$  and let  $D_m$  be the dihedral group of order  $n$  — the set of symmetries of a regular  $m$ -gon.  $D_m$  has property  $\#$  if and only if 2 is the prime (or one of the primes) with greatest power in the prime power expansion of  $n$ .

Proof. Continue to assume  $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ , with  $n_1 \geq n_i$  for  $i = 1, 2, 3, \dots, k$ . If  $p_1 = 2$ , then  $D_m$  has property  $\#$  because the subgroup of all rotations  $\langle R_{\frac{360}{m}} \rangle$  is isomorphic to  $\mathbb{Z}_m = \mathbb{Z}_{n/2} = \mathbb{Z}_{n/p_1}$ . Otherwise,  $p_1 \neq 2$  and  $n_1$  is greater than the power of 2 in the prime power expansion of  $n$ . Then  $D_m$  would have property  $\#$  provided that there is a copy of  $\mathbb{Z}_{n/p_1}$  contained in  $D_m$ , or, equivalently, that there is an element of order  $n/p_1$  in  $D_m$ . If this element is a reflection, it has order 2 and  $n = 2p_1$  — a contradiction since we can choose the power of  $p_1$  is not greater than the power of 2. If the element is a rotation, then it is contained in  $\langle R_{\frac{360}{m}} \rangle$ , a cyclic subgroup of order  $m$  and  $n/p_1 = 2m/p_1$  divides  $m$ . So, for some  $q$ ,

$$\begin{aligned}
m &= (2m/p_1)q \\
\Rightarrow mp_1 &= 2qm \\
\Rightarrow p_1 &= 2q.
\end{aligned}$$

This contradicts the assumption that  $p_1$  is a prime and not equal to 2, so  $D_m$  does not have property # when another prime's power exceeds that of 2 in the prime power expansion of  $n = 2m$ .  $\diamond$

## 5 Symmetric Groups

In the next three examples, we consider symmetric groups, which lead us to another general result.

Example 8. The symmetric group  $S_3$  has order  $6 = 2 \cdot 3$ , so, using the convention above,  $p_1 = 2$  or  $p_1 = 3$ . Any two-cycle has order  $2 = 6/3 = n/p_1$  and any three-cycle has order  $3 = 6/2 = n/p_1$ . By the corollary to Theorem 2,  $S_3$  has property #.

Example 9. The order of the symmetric group  $S_4$  is  $24 = 2^3 \cdot 3$ . Property # would require an element of order  $24/2 = 12$ , but elements in  $S_4$  are either the identity, two-cycles, a product of disjoint two-cycles, three-cycles, or four-cycles. Neither of these has order 12, so  $S_4$  does not have property #.

Example 10.  $S_5$  has order  $5! = 120 = 2^3 \cdot 3 \cdot 5$ , so  $n/p_1 = 120/2 = 60$ . Elements in  $S_5$  have order at most 6 (the product of a two-cycle and a disjoint three-cycle), so  $S_5$  does not have property #.

Theorem 5.  $S_m$  does not have property # when  $m \geq 4$ .

Proof. Let  $n = m! = |S_m|$  where  $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ , with  $n_1 \geq n_i$  for  $i = 1, 2, 3, \dots, k$ .

First, we show that  $p_1$  must equal 2. Intuitively, more factors of 2 appear in  $m!$  than of other primes since 2 is a divisor of every other integer from 1 to  $m$ , while other primes divide fewer of those integers. To verify the conclusion more technically, suppose for a given prime  $p$  that  $p^s \leq m < p^{s+1}$ . We proceed to find the exponent of  $p$ , call it  $n(p)$ , in the prime power of expansion of  $n = m!$ . There are  $\lfloor \frac{m}{p} \rfloor$  multiples of  $p$  less than  $m$ , so  $n(p) \geq \lfloor \frac{m}{p} \rfloor$ . Next, there are  $\lfloor \frac{m}{p^2} \rfloor$  multiples of  $p^2$  less than or equal to  $m$ , each of which adds another factor of  $p$  to  $n = m!$ . So far,

$$n(p) \geq \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor$$

Likewise, we may continue to count the factors of powers of  $p$  in  $n = m!$  until we reach  $p^s$ . This gives

$$n(p) = \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \dots + \lfloor \frac{m}{p^s} \rfloor.$$

Since  $p \geq 2$  for all primes  $p$ ,  $n(p) \leq n(2)$ . Therefore, 2 is the prime with the greatest power in the prime-power expansion of  $n$ , that is  $p_1 = 2$ .

Next, suppose that there is an element in  $S_m$  with order  $n/p_1 = n/2 = m!/2$ . This element can be written as the product of  $r$  disjoint cycles of orders  $m_1, m_2, \dots, m_r$  so that

$$m_1 + m_2 + \dots + m_r \leq m \quad \text{and} \quad \text{lcm}(m_1, m_2, \dots, m_r) = \frac{m!}{2}$$

Since  $2^{n_1}$  divides  $m!$ ,  $2^{n_1-1}$  divides  $m!/2$ . In order for the factor  $2^{n_1-1}$  to appear as the least common multiple of the  $m_i$ 's, it must divide at least one of the  $m_i$ 's, and so  $2^{n_1-1} \leq m$ .

Now, we demonstrate that this is impossible for  $m \geq 6$  with a proof by induction that  $2^{n_1-1} > m$  for  $m \geq 6$ .

Base step: For  $m = 6$ ,  $n = 6! = 720 = 2^4 \cdot 3^2 \cdot 5$  and  $n_1 = 4$ . Indeed,  $2^{4-1} = 2^3 = 8 > 6$ .

Induction hypothesis: Suppose  $2^{n_1-1} > m$  for some  $m \geq 6$ .

Induction step: Let  $2^s$  be the greatest power of 2 that divides  $m + 1$ . Multiplying  $m!$  by  $m + 1$  adds a factor of  $2^s$  to  $2^{n_1}$ , and we must show that  $2^{n_1-1+s} > m + 1$ .

Well, if  $m + 1$  is even, then  $s \geq 1$ . This means that

$$2^{n_1-1+s} \geq 2^{n_1} = 2^{n_1-1} + 2^{n_1-1} > m + 2^{n_1-1} \leq m + 1$$

Otherwise,  $m + 1$  is odd and  $s = 0$ . By the induction hypothesis,  $2^{n_1-1} > m$ , which implies  $2^{n_1-1} \geq m + 1$ .

But  $m + 1$  is odd, so  $2^{n_1-1} \neq m + 1$ . Hence,  $2^{n_1-1+s} = 2^{n_1-1} > m + 1$ .



Therefore, it is impossible for  $S_m$  to contain an element of order  $m!/2$  when  $m \geq 6$ ,  $m = 4$  (Example 9), or  $m = 5$  (Example 10); consequently,  $S_m$  does not have property  $\#$  when  $m \geq 4$ .  $\diamond$

## 6 Conclusion

Recall the original problem: In a group  $G$  of order 65, let  $a$  and  $b$  be nonidentity elements of different orders and prove that no proper subgroup of  $G$  contains  $a$  and  $b$ . A “new” solution that applies the ideas of this paper may be:  $65 = 5 \cdot 13$  and  $b_{65} = 1(1 + 1) - 1 = 1$ . For a proper subgroup  $H$  of  $G$ ,  $\text{odim}(H) \leq b_{65} = 1$  (Theorem 1) so no proper subgroup of  $G$  can contain two nonidentity elements of different orders. However,  $G$  has property  $\#$ . By Cauchy’s Theorem,  $G$  contains at least one element of order 13 and at least one of order 5 that each generate cyclic subgroups isomorphic to  $\mathbb{Z}_{13} = \mathbb{Z}_{65/5}$  and  $\mathbb{Z}_5 = \mathbb{Z}_{65/13}$ , respectively. Both 5 and 13 have the greatest powers in the prime power expansion of  $|G| = 65$ ; therefore, by the corollary to Theorem 2, any group of order 65 has property  $\#$ .

Although it is not likely to be found in an Abstract Algebra text, a more general version of the original problem is: Let  $G$  be a group of order  $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ , where  $n_1 \geq n_i$  for  $i = 1, 2, 3, \dots, k$ . Show that the only subgroup of  $G$  that contains a collection  $S$  of  $n_1(n_2 + 1) \dots (n_k + 1)$  nonidentity elements of different orders is  $G$  itself. Solution: Suppose a subgroup  $H$  of  $G$  contains  $S$ . Then  $\text{odim}(H) \geq n_1(n_2 + 1) \dots (n_k + 1) = b_n + 1 > b_n$  and by Theorem 1,  $H$  cannot be proper. It follows that  $H = G$ .