Abelian SP-Groups

Chad T. Lower

Dr. Lenny Jones, Advisor

Abstract

Let G be a finite group and let d be a divisor of $|G|$. Define n_d to be the number of subgroups of G of order d. We call G a *subgroup-perfect group*, denoted SP-Group, if, for every divisor d of $|G|$ with $n_d \neq 0$, n_d divides $|G|$. The authors investigate abelian SP-groups. (Chad T. Lower and Lenny Jones)

1. INTRODUCTION Mathematicians and nonmathematicians have been fascinated for centuries by the properties and patterns of numbers. It is this curiosity that prompted the authors to look at patterns within finite groups. Specifically, we are interested in finding out the number of groups that have the property of having the number of subgroups of the group with a certain order dividing the order of the group. Our initial assessment leads us to believe that there are an infinite number of such groups and we will attempt to find all of them.

We start by looking at finite abelian groups. A group is a finite or infinite set of elements together with a binary operation which together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property. An abelian group is defined to be a group for which the elements commute (i.e. $AB = BA$ for all elements A and B in the group). A finite group is a group containing a finite number of elements. By computing the characteristic factors, any abelian group can be expressed as a group direct product of cyclic subgroups. It is these cyclic subgroups that we will be focusing our attention on.

2. PRELIMINARIES Throughout this article, G will be a finite abelian group and $|G|$ will denote its cardinality.

Definition 1. Let d be a divisor of $|G|$. We define n_d to be the number of subgroups of G with order d.

Definition 2. A group G is said to be a **subgroup-perfect group**, denoted ***SP*-Group**, if, for every divisor d of $|G|$ with $n_d \neq 0$, n_d divides $|G|$.

Definition 3. Let x be a positive integer and let p be a prime number. We define

$$(\mathbb{Z}_p)^x = \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{x\text{-factors}}.$$

Example 1. *(Trivial Case) Let $G = \mathbb{Z}_m$ where m is a positive integer. G is a finite, cyclic abelian group. For any divisor d of G, $n_d = 1$. Therefore, G is an SP-Group.*

Example 2. *Let $G = \mathbb{Z}_6 \times \mathbb{Z}_6 \simeq (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2$. Then $|G| = 36$. Divisors of $|G|$ are 1, 2, 3, 4, 6, 9, 12, 18, and 36. G is an SP-Group (as indicated by the following table) since n_d divides $|G|$ for all values of d.*

d	n_d	*subgroups of G with order d*
1	1	$\langle(0,0)\rangle$
2	3	$\langle(0,3)\rangle$, $\langle(3,0)\rangle$, $\langle(3,3)\rangle$
3	4	$\langle(0,2)\rangle$, $\langle(2,0)\rangle$, $\langle(2,2)\rangle$, $\langle(2,4)\rangle$
4	1	$\langle(0,3),(3,0)\rangle$
6	12	$\langle(0,1)\rangle$, $\langle(1,0)\rangle$, $\langle(1,1)\rangle$, $\langle(1,2)\rangle$, $\langle(1,3)\rangle$, $\langle(1,4)\rangle$, $\langle(1,5)\rangle$, $\langle(2,1)\rangle$, $\langle(2,3)\rangle$, $\langle(2,5)\rangle$, $\langle(3,1)\rangle$, $\langle(3,2)\rangle$
9	1	$\langle(0,2),(2,0)\rangle$
12	4	$\langle(0,3),(1,0)\rangle$, $\langle(2,1),(3,0)\rangle$, $\langle(3,0),(4,1)\rangle$, $\langle(0,1),(3,0)\rangle$
18	3	$\langle(0,1),(2,0)\rangle$, $\langle(0,2),(1,0)\rangle$, $\langle(1,1),(2,0)\rangle$
36	1	G

Example 3. *Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then $|G| = 4$. Divisors of $|G|$ are 1, 2, and 4. So G is not an SP-Group (as indicated by the following table) since $n_2 = 3$ does not divide $|G|$.*

d	n_d	*subgroups of G with order d*
1	1	$\langle(0,0)\rangle$
2	3	$\langle(0,1)\rangle$, $\langle(1,0)\rangle$, $\langle(1,1)\rangle$
4	1	G

Example 4. *Let* $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ *(*NOTE: *S_3 is not an abelian group but used to show a non-abelian example of an SP-Group). Observe that* $|S_3| = 6$. *Possible values of* d *are 1, 2, 3, and 6. Then* S_3 *is an SP-Group as indicated by the following table:*

d	n_d	*subgroups of* G *with order* d
1	*1*	$\langle(1)\rangle$
2	*3*	$\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$
3	*1*	$\langle(123)\rangle$
6	*1*	S_3

Proposition 1. *Let* $G \simeq (\mathbb{Z}_p)^x$ *where* p *is prime. The number of subgroups of order* p^a, *where* $1 \leq a \leq x$ *is defined as*

$$n_{p^a} = \prod_{j=1}^{a} \frac{p^{x-j+1} - 1}{p^j - 1}.$$

Proof: See [1]. ■

Proposition 2. *Let* $G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y$ *where* p *and* q *are distinct primes. The number of subgroups of order* $p^a q^b$ *can be found by multiplying the number of subgroups of order* p^a *and the number of subgroups of* q^b *since* p^a *and* q^b *are relatively prime. We find*

$$n_{p^a q^b} = n_{p^a} \cdot n_{q^b}.$$

Proposition 3 (Trivial Case)**.** *Let* $G \simeq \mathbb{Z}_p \times \mathbb{Z}_q$, *where* p *and* q *are distinct primes. Then* G *is an SP-group.*

Proof: The proof can be seen as a specialized case of Example 1 and Proposition 2. ■

Theorem 1. *If* $G \simeq (\mathbb{Z}_{p^n})^2 = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$, *where* p *is prime, then* G *is not an SP-group for any positive integer* n.

Proof: G has $(p^n)^2 = p^{2n}$ elements and has subgroups of order $p^0 = 1$, $p^1 = p$, p^2, ..., p^{2n-1}, and p^{2n}. The number of subgroups of order p is

$$n_p = 2p - 1,$$

which will never divide p^{2n} since $p < 2p-1 < 2p$ for all primes p, but all divisors of p^{2n} will be of the form kp for some $k \in \mathbb{Z}$. In reality, k must be some power of p. ■

Looking at the case $G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y$, where p and q are distinct primes, $p < q$, and at least one of x and y is > 1, there are three cases that can occur. Our three cases that can occur are when $x = y$, $x < y$, and $x > y$. Let us begin with the case when $x = y$.

Proposition 4. *Let $G \simeq (\mathbb{Z}_p)^2 \times (\mathbb{Z}_q)^2$, where p and q are distinct primes with $p < q$. Then G is an* SP*-group if and only if $p = 2$ and $q = 3$.*

Proof: We know $|G| = p^2q^2$. The number of subgroups of order $p^0 = 1$, p^2, $q^0 = 1$, and q^2 equals 1 and 1 will always divide $|G|$. Also, from Proposition 2, the number of subgroups of order p^2q^2 equals 1, which will always divide $|G|$. Ignoring these trivial cases, we look at the number of subgroups of order $p^1 = p$ $(= pq^2$ by Proposition 2), $q^1 = q$ $(= p^2q$ by Proposition 2), and pq.

$$n_p = \prod_{j=1}^{1} \frac{p^{2-j+1}-1}{p^j-1} = \frac{p^2-1}{p-1} = p+1.$$

$$n_q = \prod_{j=1}^{1} \frac{q^{2-j+1}-1}{q^j-1} = \frac{q^2-1}{q-1} = q+1.$$

$$n_{pq} = n_p n_q = (p+1)(q+1) \text{ (by Proposition 2).}$$

To be an *SP*-group, $(p+1)|p^2q^2$, $(q+1)|p^2q^2$, and $(p+1)(q+1)|p^2q^2$. We will look at these conditions individually starting with $(p+1)|p^2q^2$. Since $(p+1)$ cannot divide p^2 or p, then $(p+1)|q^2$ in order for G to be an *SP*-group. Similarly, $(q+1)|p^2$. (NOTE: We can ignore the case when $(p+1)(q+1)|p^2q^2$ since it is equivalent to say $(p+1)|q^2$ and $(q+1)|p^2$. These two cases are being considered in n_p and n_q.) Since $p < q$, we know q is odd, so p^2 and hence p must be even. Therefore, $p = 2$. Since $p = 2$, then $(q+1)|4$ and $q = 3$. Example 2 works out the specifics for how this is an *SP*-Group. Therefore, $G \simeq (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2$ is the only *SP*-group of this form. ■

Proposition 5. *Let $G \simeq (\mathbb{Z}_p)^3 \times (\mathbb{Z}_q)^3$, where p and q are distinct primes with $p < q$. Then G is not an SP-group.*

Proof: We know $|G| = p^3q^3$. The number of subgroups of order q is

$$n_q = \prod_{j=1}^{1} \frac{q^{3-j+1}-1}{q^j-1} = \frac{q^3-1}{q-1} = q^2+q+1.$$

We know p^3 has 4 divisors: 1, p, p^2, and p^3. In order for $q^2+q+1|p^3$, q^2+q+1 must equal one of the divisors of p^3. We know q^2+q+1 cannot equal 1, p, or p^2 since $p < q$. So $q^2+q+1 = p^3$. We can also show that the number of subgroups of order p is

$$n_p = \prod_{j=1}^{1} \frac{p^{3-j+1}-1}{p^j-1} = \frac{p^3-1}{p-1} = p^2+p+1.$$

Since p^2+p+1 must divide q^3, then either $p^2+p+1 = q$, $p^2+p+1 = q^2$, or $p^2+p+1 = q^3$. If $p^2+p+1 = q$ then $q^2+q+1 = p^3$ can be rewritten as $(p^2+p+1)^2+(p^2+p+1)+1 = p^3$ or $p^4+2p^3+4p^2+4p+2 = p^3$ which is impossible. If $p^2+p+1 = q^2$ then $q^2+q+1 = p^3$ can be rewritten as $(p^2+p+1)^2+q+1 = p^3$ or $q = -p^4-p^3-3p^2-2p-2$ which is impossible. If $p^2+p+1 = q^3$ then $q^2+q+1 = p^3$ can be rewritten as $q^2+q = (p-1)(q^3)$ or $\frac{1}{q}+\frac{1}{q^2}+1 = p$ which is impossible. Therefore, no such p and q exist so that G is an *SP*-group. ■

Proposition 6. *Let $G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^x$, where p and q are distinct primes with $p < q$ and $x \geq 4$. Then G is not an SP-group.*

Proof: We know $|G| = p^xq^x$. For all values of $x > 3$, the number of subgroups of order q^2 is

$$n_{q^2} = \prod_{j=1}^{2} \frac{q^{x-j+1}-1}{q^j-1} = \frac{(q^x-1)(q^{x-1}-1)}{(q-1)(q^2-1)}.$$

To be an *SP*-group, n_{q^2} must divide p^x. When x is odd,

$$n_{q^2} = (q^{x-1}+q^{x-2}+\cdots+q+1)(q^{x-3}+q^{x-5}+\cdots+q^2+1),$$

but $n_{q^2} > p^x$ since $p < q$. When x is even,

$$n_{q^2} = (q^{x-2}+q^{x-3}+\cdots+q+1)(q^{x-2}+q^{x-4}+\cdots+q^2+1),$$

but $n_{q^2} > p^x$ since $p < q$. Therefore, no such p and q exist so that G is an *SP*-group. ■

To summarize the previous:

Theorem 2. *Let $G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^x$, where p and q are distinct primes with $p < q$. Then G is an SP-group if and only if $x = 1$ and p, q are prime or $x = 2$ and $p = 2$, $q = 3$.*

Next, let's look at the case when $x < y$.

Theorem 3. *Let $G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y$, where p and q are distinct primes with $p < q$ and x and y are positive integers with $x < y$. Then G is not an SP-group.*

Proof: We know $|G| = p^x q^y$. For all values of x and y, with $x < y$, the number of subgroups of order q is

$$n_q = \prod_{j=1}^{1} \frac{q^{y-j+1} - 1}{q^j - 1} = \frac{q^y - 1}{q - 1} = q^{y-1} + q^{y-2} + \cdots + q + 1.$$

To be an *SP*-group, n_q must divide p^x. But $n_q > q^x > p^x$ since $p < q$ and $x < y$. Therefore, no such p and q exist so that G is an *SP*-group. ■

Next, let's look at the case when $x > y$.

Proposition 7. *Let $G \simeq (\mathbb{Z}_p)^2 \times \mathbb{Z}_q$, where p and q are distinct primes with $p < q$. Then G is an* SP*-group if and only if $p = 2$ and $q = 3$.*

Proof: We know $|G| = p^2 q$. The number of subgroups of order 1, p^2, q and $p^2 q$ equals 1 and 1 will always divide $|G|$. (NOTE: We can also ignore the case when the number of subgroups is pq since $n_p = n_{pq}$.) The number of subgroups of order p is

$$n_p = \prod_{j=1}^{1} \frac{p^{2-j+1} - 1}{p^j - 1} = \frac{p^2 - 1}{p - 1} = p + 1.$$

To be an *SP*-group, $n_p = p + 1$ must divide q. But since q is prime, it has only 2 divisors. So $p + 1 = q$. Since $p < q$, we know q is odd, so p must be even. Therefore, $p = 2$. Since $p + 1 = q$, $q = 3$. It can easily be shown that this case does make an *SP*-group. Therefore, $G \simeq (\mathbb{Z}_2)^2 \times \mathbb{Z}_3$ is the only *SP*-group of this form. ■

Proposition 8. *Let $G \simeq (\mathbb{Z}_p)^3 \times \mathbb{Z}_q$, where p and q are distinct primes with $p < q$. Then G is an* SP*-group if and only if $p^2 + p + 1 = q$.*

Proof: We know $|G| = p^3q$. The number of subgroups of order 1, p^3, q and p^3q equals 1 and 1 will always divide $|G|$. (NOTE: We can ignore the case when the number of subgroups is p^2 since $n_p = n_{p^2}$. Also, pq and p^2q can be ignored since $n_p = n_{pq} = n_{p^2q}$.) The number of subgroups of order p is

$$n_p = \prod_{j=1}^{1} \frac{p^{3-j+1} - 1}{p^j - 1} = \frac{p^3 - 1}{p - 1} = p^2 + p + 1.$$

To be an *SP*-group, $n_p = p^2 + p + 1$ must divide q. But since q is prime, it has only 2 divisors. So $p^2 + p + 1 = q$. For p and q values that satisfy this condition, it is easily shown that each case is an *SP*-Group. ■

The following example shows that the prime numbers 2 and 7 satisfy this condition and are an SP-group.

Example 5. *Let $G \simeq (\mathbb{Z}_2)^3 \times \mathbb{Z}_7$. Then $|G| = 56$. Divisors of $|G|$ are 1, 2, 4, 7, 8, 14, 28, and 56. So G is an SP-Group (as indicated by the following table) since n_d divides $|G|$ for all values of d. [GAP was used to assist in the creation of this table.]*

d	n_d	*subgroups of G with order d*
1	1	$\langle(0,0,0,0)\rangle$
2	7	$\langle(0,0,1,0)\rangle$, $\langle(0,1,0,0)\rangle$, $\langle(0,1,1,0)\rangle$, $\langle(1,0,0,0)\rangle$, $\langle(1,0,1,0)\rangle$, $\langle(1,1,0,0)\rangle$, $\langle(1,1,1,0)\rangle$
4	7	$\langle(0,0,1,0),(0,1,0,0)\rangle$, $\langle(0,0,1,0),(1,0,0,0)\rangle$, $\langle(0,1,0,0),(1,0,0,0)\rangle$, $\langle(0,0,1,0),(1,1,0,0)\rangle$, $\langle(0,1,0,0),(1,0,1,0)\rangle$, $\langle(1,0,0,0),(0,1,1,0)\rangle$, $\langle(0,1,1,0),(1,1,0,0)\rangle$
7	1	$\langle(0,0,0,1)\rangle$
8	1	$\langle(0,0,1,0),(0,1,0,0),(1,0,0,0)\rangle$
14	7	$\langle(0,0,1,0)(0,0,0,1)\rangle$, $\langle(0,1,0,0),(0,0,0,1)\rangle$, $\langle(0,1,1,0),(0,0,0,1)\rangle$, $\langle(1,0,0,0),(0,0,0,1)\rangle$, $\langle(1,0,1,0),(0,0,0,1)\rangle$, $\langle(1,1,0,0),(0,0,0,1)\rangle$, $\langle(1,1,1,0),(0,0,0,1)\rangle$
28	7	$\langle(0,0,1,0),(0,1,0,0),(0,0,0,1)\rangle$, $\langle(0,0,1,0),(1,0,0,0),(0,0,0,1)\rangle$, $\langle(0,1,0,0),(1,0,0,0),(0,0,0,1)\rangle$, $\langle(0,0,1,0),(1,1,0,0),(0,0,0,1)\rangle$, $\langle(0,1,0,0),(1,0,1,0),(0,0,0,1)\rangle$, $\langle(1,0,0,0),(0,1,1,0),(0,0,0,1)\rangle$, $\langle(0,1,1,0),(1,1,0,0),(0,0,0,1)\rangle$
56	1	G

Other values of p and q that will work are when p equals 3, 5, 17, 41, 59, 71, 89, 101, and 131 when their respective q values are 13, 31, 307, 1723, 3541, 5113, 8011, 10303, and 17293. A conjecture has been made that there may be an infinite number of primes that meet the condition $p^2 + p + 1 = q$.

Proposition 9. *Let $G \simeq (\mathbb{Z}_p)^x \times \mathbb{Z}_q$, where p and q are distinct primes with $p < q$ and $x \geq 4$. Then G is not an SP-group.*

Proof: We know $|G| = p^x q$. For all values of x greater than three, the number of subgroups of order p is

$$n_p = \prod_{j=1}^{1} \frac{p^{x-j+1} - 1}{p^j - 1} = \frac{p^x - 1}{p - 1} = p^{x-1} + p^{x-2} + \cdots + p + 1.$$

and number of subgroups of order p^2 is

$$n_{p^2} = \prod_{j=1}^{2} \frac{p^{x-j+1} - 1}{p^j - 1} = \frac{(p^x - 1)(p^{x-1} - 1)}{(p - 1)(p^2 - 1)}.$$

To be an *SP*-group, n_p and n_{p^2} must divide q. But since q is prime, it has only 2 divisors. So $n_p = q$ and $n_{p^2} = q$. Since n_p and n_{p^2}, both equal q, they must equal each other, so $n_p = n_{p^2}$. When x is odd, this implies $p^{x-1}+p^{x-2}+\cdots+p+1 = (p^{x-1}+p^{x-2}+\cdots+p+1)(p^{x-3}+p^{x-5}+\cdots+p^2+1)$, or $1 = p^{x-3}+p^{x-5}+\cdots+p^2+1$, which is a contradiction. When x is even, this implies $p^{x-1}+p^{x-2}+\cdots+p+1 = (p^{x-2}+p^{x-3}+\cdots+p+1)(p^{x-2}+p^{x-4}+\cdots+p^2+1)$, or $p^{x-3} = (p^{x-2} + p^{x-3} + \cdots + p + 1)(p^{x-4} + p^{x-6} + \cdots + p^2 + 1)$ which is a contradiction. Therefore, no such p and q exist so that G is an *SP*-group when $x \geq 4$ and $y = 1$. ■

To summarize the previous:

Theorem 4. *Let $G \simeq (\mathbb{Z}_p)^x \times \mathbb{Z}_q$, where p and q are distinct primes and $x \geq 2$. Then G is an SP-group if and only if $x = 2$ and $p = 2$, $q = 3$ or $x = 3$ and p, q are primes that satisfy the equation $p^2 + p + 1 = q$.*

Proposition 10. *Let $G \simeq (\mathbb{Z}_p)^3 \times (\mathbb{Z}_q)^2$, where p and q are distinct primes with $p < q$. Then G is an* SP*-group if and only if $p = 2$ and $q = 7$.*

Proof: We know $|G| = p^3 q^2$. Again, ignoring the trivial and repeat cases, we know that the number of subgroups of order p is

$$n_p = \prod_{j=1}^{1} \frac{p^{3-j+1} - 1}{p^j - 1} = \frac{p^3 - 1}{p - 1} = p^2 + p + 1.$$

The number of subgroups of order q is

$$n_q = \prod_{j=1}^{1} \frac{q^{2-j+1}-1}{q^j-1} = \frac{q^2-1}{q-1} = q+1.$$

To be an *SP*-group, $n_p = p^2+p+1$ must divide q^2 and $n_q = q+1$ must divide p^3. Since $p < q$, we know q is odd, so p must be even. Therefore, $p = 2$. Since $p^2+p+1 = 7$ must divide q^2, $q = 7$. We know $q+1 = 8$ must divide $p^3 = 8$, and 8 does divide 8. It can easily be shown that this case does make an *SP*-group. Therefore, $G \simeq (\mathbb{Z}_2)^3 \times (\mathbb{Z}_7)^2$ is the only *SP*-group of this form.■

Proposition 11. *Let $G \simeq (\mathbb{Z}_p)^4 \times (\mathbb{Z}_q)^y$, where p and q are distinct primes with $p < q$ and $y < 4$. Then G is not an* SP*-group.*

Proof: We know $|G| = p^4q^y$. For $x = 4$, the number of subgroups of order p is

$$n_p = \prod_{j=1}^{1} \frac{p^{4-j+1}-1}{p^j-1} = \frac{p^4-1}{p-1} = p^3+p^2+p+1.$$

To be an *SP*-group, $n_p = p^3+p^2+p+1$ must divide q^y. Since $p < q$, we know q is odd, so p must be even. Therefore, $p = 2$. Since $p^3+p^2+p+1 = 15$, then 15 must divide q^y. But this is impossible if q is prime. Therefore, no such p and q exist so that G is an *SP*-group when $x = 4$ and $y < 4$. ■

Proposition 12. *Let $G \simeq (\mathbb{Z}_p)^5 \times (\mathbb{Z}_q)^y$, where p and q are distinct primes with $p < q$ and $y < 5$. Then G is not an* SP*-group.*

Proof: We know $|G| = p^5q^y$. For $x = 5$, the number of subgroups of order p^2 is

$$n_{p^2} = \prod_{j=1}^{2} \frac{p^{5-j+1}-1}{p^j-1} = \frac{(p^5-1)(p^4-1)}{(p-1)(p^2-1)} = (p^2+1)(p^4+p^3+p^2+p+1).$$

To be an *SP*-group, $n_p^2 = (p^2+1)(p^4+p^3+p^2+p+1)$ must divide q^y. Since $p < q$, we know q is odd, so p must be even. Therefore, $p = 2$. Since $(p^2+1)(p^4+p^3+p^2+p+1) = 155$, then 155 must divide q^y. But this is impossible if q is prime. Therefore, no such p and q exist so that G is an *SP*-group when $x = 5$ and $y < 5$. ■

Proposition 13. *Let $G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y$, where p and q are distinct primes with $p < q$ and $x \geq 4$. Then G is not an SP-group. (*NOTE: *This proposition can be an alternate proof for Propositions 6, 9, 11, and 12.)*

Proof: We know $|G| = p^x q^y$. For all values of $x \geq 4$, the number of subgroups of order p^2 is

$$n_{p^2} = \prod_{j=1}^{2} \frac{p^{x-j+1} - 1}{p^j - 1} = \frac{(p^x - 1)(p^{x-1} - 1)}{(p-1)(p^2 - 1)}. \tag{1}$$

To be an *SP*-group, n_{p^2} must divide q^y. The largest irreducible polynomial factor of $p^x - 1$ is $\Phi_x(p)$, the x^{th} cyclotomic polynomial. The degree of $\Phi_x(p)$ is $\phi(x)$, where ϕ is Euler's totient. Similarly, the largest irreducible polynomial factor of $p^{x-1} - 1$ is $\Phi_{x-1}(p)$, and its degree is $\phi(x-1)$. For $x \geq 4$, both $\phi(x)$ and $\phi(x-1)$ are larger than one. Hence, both $\Phi_x(p)$ and $\Phi_{x-1}(p)$ remain factors of the numerator of (1) after performing the division. Consequently, $\Phi_x(p)$ and $\Phi_{x-1}(p)$ must both divide q^y and so q divides both $\Phi_x(p)$ and $\Phi_{x-1}(p)$. Then q divides both $p^x - 1$ and $p^{x-1} - 1$. But then q also divides the difference $(p^x - 1) - (p^{x-1} - 1) = p^{x-1}(p-1)$. Since q cannot divide p^{x-1}, it must divide $p - 1$, but this is impossible since $p < q$. Therefore, no such p and q exist so that G is an *SP*-group. ■

Theorem 5. *Let $G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y$, where p and q are distinct primes with $p < q$ and x and y are positive integers with $x > y$. Then G is an SP-group if and only if $x = 3$, $y = 1$, and $p^2 + p + 1 = q$ when p, q are prime or $x = 3$, $y = 2$, $p = 2$, and $q = 7$.*

Looking graphically at all the cases that have either been found (O) or have been disproved (X), we see all cases of $(\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y$ have been shown when using two distinct primes p and q.

$y \diagdown x$	1	2	3	4	5	6	7	8	9	10	...
1	O	O	O	X	X	X	X	X	X	X	X
2	X	O	O	X	X	X	X	X	X	X	X
3	X	X	X	X	X	X	X	X	X	X	X
4	X	X	X	X	X	X	X	X	X	X	X
5	X	X	X	X	X	X	X	X	X	X	X
6	X	X	X	X	X	X	X	X	X	X	X
7	X	X	X	X	X	X	X	X	X	X	X
8	X	X	X	X	X	X	X	X	X	X	X
9	X	X	X	X	X	X	X	X	X	X	X
10	X	X	X	X	X	X	X	X	X	X	X
...	X	X	X	X	X	X	X	X	X	X	X

More specifically, the trivial case ($G \simeq \mathbb{Z}_p \times \mathbb{Z}_q$) has an infinite number of solutions. The cases when $G \simeq (\mathbb{Z}_p)^2 \times \mathbb{Z}_q$ and $G \simeq (\mathbb{Z}_p)^2 \times (\mathbb{Z}_q)^2$ both have a unique solutions when $p = 2$ and $q = 3$. The case when $G \simeq (\mathbb{Z}_p)^3 \times (\mathbb{Z}_q)^2$ has a unique solution when $p = 2$ and $q = 7$. Finally, the case when $G \simeq (\mathbb{Z}_p)^3 \times \mathbb{Z}_q$ has solutions when $p^2 + p + 1 = q$. There may be an infinite number of *SP*-groups that meet this last criteria.

We have started examining cases that involve more that two prime numbers, i.e. when

$$G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y \times (\mathbb{Z}_r)^z \text{ and}$$

$$G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y \times (\mathbb{Z}_r)^z \times (\mathbb{Z}_s)^w.$$

Looking at the case $G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y \times (\mathbb{Z}_r)^z$, where p, q, and r are distinct primes, $p < q < r$, and at least one of x, y and z is > 1, there are many cases that can occur. We will begin by looking at the case when $x = y = z$.

Proposition 14 (Trivial Case)**.** *Let $G \simeq \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$, where p, q, and r are distinct primes. Then G is an SP-group.*

Proof: The proof can be seen as a specialized case of Example 1. ■

Proposition 15. *Let $G \simeq (\mathbb{Z}_p)^2 \times (\mathbb{Z}_q)^2 \times (\mathbb{Z}_r)^2$, where p, q, and r are distinct primes with $p < q < r$. Then G is an* SP*-group if and only if $p = 2$, $q = 3$, and $r = 5$, 11, or 17.*

Proof: We know $|G| = p^2q^2r^2$. Ignoring the trivial cases, we look at the number of subgroups of order p, q, and r.

$$n_p = \prod_{j=1}^{1} \frac{p^{2-j+1}-1}{p^j-1} = \frac{p^2-1}{p-1} = p+1.$$

$$n_q = \prod_{j=1}^{1} \frac{q^{2-j+1}-1}{q^j-1} = \frac{q^2-1}{q-1} = q+1.$$

$$n_r = \prod_{j=1}^{1} \frac{r^{2-j+1}-1}{r^j-1} = \frac{r^2-1}{r-1} = r+1.$$

To be an *SP*-group, $(p+1)|q^2r^2$, $(q+1)|p^2r^2$, and $(r+1)|p^2q^2$. Since $r > q > p$, we know r and q are odd, so p^2 and hence p must be even so $p = 2$. Since $p = 2$, then $3|q^2r^2$, $q+1|4r^2$, and $r+1|4q^2$. Since $q < r$ and $3|q^2r^2$, $q = 3$. Now we have $3|9r^2$, $4|4r^2$, and $r+1|4 \cdot 9 = 36$. The first two equations will be true for all primes $r > 3$. In order for $r+1|36$, r can be 5, 11, or 17 since $6|36$, $12|36$, and $18|36$ respectively. It can easily be shown that these cases make an *SP*-group. Therefore, $G_1 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2$, $G_2 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{11})^2$, and $G_3 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{17})^2$ are the only *SP*-groups of this form. ■

Proposition 16. *Let $G \simeq (\mathbb{Z}_p)^2 \times (\mathbb{Z}_q)^2 \times \mathbb{Z}_r$, where p, q, and r are distinct primes with $p < q < r$. Then G is an* SP*-group if and only if $p = 2$ and $q = 3$.*

Proof: We know $|G| = p^2q^2r$. Ignoring the trivial cases, we look at the number of subgroups of order p, q, and r.

$$n_p = \prod_{j=1}^{1} \frac{p^{2-j+1}-1}{p^j-1} = \frac{p^2-1}{p-1} = p+1.$$

$$n_q = \prod_{j=1}^{1} \frac{q^{2-j+1}-1}{q^j-1} = \frac{q^2-1}{q-1} = q+1.$$

$$n_r = \prod_{j=1}^{1} \frac{r^{1-j+1}-1}{r^j-1} = \frac{r^1-1}{r-1} = 1.$$

To be an *SP*-group, $(p+1)|q^2r$, $(q+1)|p^2r$, and $1|p^2q^2$ (this third condition will always be true). Since $r > q > p$, we know r and q are odd, so p^2 and hence p must be even so $p = 2$. Since $p = 2$, then $3|q^2r$ and $q+1|4r$. Since $q < r$ and $3|q^2r$, $q = 3$. Now we have $3|9r$ and $4|4r$. The first two equations will be true for all primes $r > 3$ and it can easily be shown that these cases

do make *SP*-groups. Therefore, all groups of the form $G \simeq (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times \mathbb{Z}_r$ for r being any prime are *SP*-Groups. ■

Proposition 17. *Let $G \simeq (\mathbb{Z}_p)^2 \times (\mathbb{Z}_q)^2 \times (\mathbb{Z}_r)^3$, where p, q, and r are distinct primes with $p < q < r$. Then G is not an* SP*-group.*

Proof: We know $|G| = p^2q^2r^3$. Ignoring the trivial cases, we look at the number of subgroups of order p, q, and r.

$$n_p = \prod_{j=1}^{1} \frac{p^{2-j+1} - 1}{p^j - 1} = \frac{p^2 - 1}{p - 1} = p + 1.$$

$$n_q = \prod_{j=1}^{1} \frac{q^{2-j+1} - 1}{q^j - 1} = \frac{q^2 - 1}{q - 1} = q + 1.$$

$$n_r = \prod_{j=1}^{1} \frac{r^{3-j+1} - 1}{r^j - 1} = \frac{r^3 - 1}{r - 1} = r^2 + r + 1.$$

To be an *SP*-group, $(p+1)|q^2r^3$, $(q+1)|p^2r^3$, and $(r^2+r+1)|p^2q^2$. Since $r > q > p$, we know r and q are odd, so p^2 and hence p must be even so $p = 2$. Since $p = 2$, then $3|q^2r^3$, $q+1|4r^3$, and $r^2+r+1|4q^2$. Since $q < r$ and $3|q^2r^3$, $q = 3$. Now we have $3|9r^3$, $4|4r^3$, and $r^2 + r + 1|4 \cdot 9 = 36$. The first two equations will be true for all primes $r > 3$. To have an *SP*-group, we need to find a prime r so that $(r^2 + r + 1)|36$, but no such r exists that will make this true. Therefore, no such p, q, and r exist so that G is an *SP*-group when $x = y = 2$ and $z = 3$. ■

Proposition 18. *Let $G \simeq (\mathbb{Z}_p)^2 \times (\mathbb{Z}_q)^2 \times (\mathbb{Z}_r)^z$, where p, q, and r are distinct primes with $p < q < r$ and $z \geq 4$. Then G is not an* SP*-group.*

Proof: We know $|G| = p^2q^2r^z$. Ignoring the trivial cases, we look at the number of subgroups of order p, q, and r.

$$n_p = \prod_{j=1}^{1} \frac{p^{2-j+1} - 1}{p^j - 1} = \frac{p^2 - 1}{p - 1} = p + 1.$$

$$n_q = \prod_{j=1}^{1} \frac{q^{2-j+1} - 1}{q^j - 1} = \frac{q^2 - 1}{q - 1} = q + 1.$$

$$n_r = \prod_{j=1}^{1} \frac{r^{z-j+1}-1}{r^j-1} = \frac{r^z-1}{r-1} = r^{z-1}+r^{z-2}+\cdots+r+1.$$

We can again show $p = 2$ and $q = 3$. To have an *SP*-group, we need to find a prime r so that $(r^{z-1}+r^{z-2}+\cdots+r+1)|36$, but $(r^{z-1}+r^{z-2}+\cdots+r+1) > 36$ for all primes $r > 3$ when $z \geq 4$. Therefore, no such p, q, and r exist so that G is an *SP*-group when $x = y = 2$ and $z \geq 4$. ■

Looking at the case $G \simeq (\mathbb{Z}_p)^x \times (\mathbb{Z}_q)^y \times (\mathbb{Z}_r)^z \times (\mathbb{Z}_s)^w$, where p, q, r, and s are distinct primes, $p < q < r < s$, and at least one of x, y, z, and w is > 1, there are many cases that can occur. We will begin by looking at the case when $x = y = z = w$.

Proposition 19 (Trivial Case)**.** *Let $G \simeq \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r \times \mathbb{Z}_s$, where p, q, r, and s are distinct primes. Then G is an SP-group.*

Proof: The proof can be seen as a specialized case of Example 1. ■

Proposition 20. *Let $G \simeq (\mathbb{Z}_p)^2 \times (\mathbb{Z}_q)^2 \times (\mathbb{Z}_r)^2 \times (\mathbb{Z}_s)^2$, where p, q, r, and s are distinct primes with $p < q < r < s$. Then G is an* SP*-group if and only if $p = 2$, $q = 3$, and $r = 5$ when $s = 11$, 19, 29, 89, 149, 179, or 449, $r = 11$ when $s = 17$, 43, 131, 197, 241, or 1451, or $r = 17$ when $s = 67$, 101, 577, 1733, or 3467.*

Proof: We know $|G| = p^2q^2r^2s^2$. Ignoring the trivial cases, we look at the number of subgroups of order p, q, r, and s.

$$n_p = \prod_{j=1}^{1} \frac{p^{2-j+1}-1}{p^j-1} = \frac{p^2-1}{p-1} = p+1.$$

$$n_q = \prod_{j=1}^{1} \frac{q^{2-j+1}-1}{q^j-1} = \frac{q^2-1}{q-1} = q+1.$$

$$n_r = \prod_{j=1}^{1} \frac{r^{2-j+1}-1}{r^j-1} = \frac{r^2-1}{r-1} = r+1.$$

$$n_s = \prod_{j=1}^{1} \frac{s^{2-j+1}-1}{s^j-1} = \frac{s^2-1}{s-1} = s+1.$$

To be an *SP*-group, $(p+1)|q^2r^2s^2$, $(q+1)|p^2r^2s^2$, $(r+1)|p^2q^2s^2$, and $(s+1)|p^2q^2r^2$. Since $s > r > q > p$, we know s, r, and q are odd, so p^2 and hence p must be even so $p = 2$. Since $p = 2$, then $3|q^2r^2s^2$, $q+1|4r^2s^2$, $r+1|4q^2s^2$, and $s+1|4q^2r^2$. Since $q < r < s$ and $3|q^2r^2s^2$, $q = 3$. Now we have $3|9r^2s^2$, $4|4r^2s^2$, $r+1|4 \cdot 9s^2 = 36s^2$, and $s+1|4 \cdot 9r^2 = 36r^2$. The first two equations will be true for all primes r, $s > 3$. In order for $r+1|36s^2$, r can be 5, 11, or 17 since $6|36s^2$, $12|36s^2$, and $18|36s^2$ respectively.

Case 1. When $r = 5$, we know $s+1|900$, so s can be 11, 19, 29, 89, 149, 179, and 449 since 12|900, 20|900, 30|900, 90|900, 150|900, 180|900, and 450|900 respectively. It can easily be shown that these cases make an *SP*-group. Therefore, $G_1 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2 \times (\mathbb{Z}_{11})^2$, $G_2 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2 \times (\mathbb{Z}_{19})^2$, $G_3 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2 \times (\mathbb{Z}_{29})^2$, $G_4 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2 \times (\mathbb{Z}_{89})^2$, $G_5 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2 \times (\mathbb{Z}_{149})^2$, $G_6 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2 \times (\mathbb{Z}_{179})^2$, and $G_7 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2 \times (\mathbb{Z}_{449})^2$ are the only *SP*-groups of this form.

Case 2. When $r = 11$, we know $s+1|4356$, so s can be 17, 43, 131, 197, 241, and 1451 since 18|4356, 44|4356, 132|4356, 198|4356, 242|4356, and 1452|4356 respectively. It can easily be shown that these cases make an *SP*-group. Therefore, $G_8 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{11})^2 \times (\mathbb{Z}_{17})^2$, $G_9 = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{11})^2 \times (\mathbb{Z}_{43})^2$, $G_{10} = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{11})^2 \times (\mathbb{Z}_{131})^2$, $G_{11} = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{11})^2 \times (\mathbb{Z}_{197})^2$, $G_{12} = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{11})^2 \times (\mathbb{Z}_{241})^2$, and $G_{13} = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{11})^2 \times (\mathbb{Z}_{1451})^2$ are the only *SP*-groups of this form.

Case 3. When $r = 17$, we know $s+1|10404$, so s can be 67, 101, 577, 1733, and 3467 since 68|10404, 102|10404, 578|10404, 1734|10404, and 3468|10404 respectively. It can easily be shown that these cases make an *SP*-group. Therefore, $G_{14} = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{17})^2 \times (\mathbb{Z}_{67})^2$, $G_{15} = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{17})^2 \times (\mathbb{Z}_{101})^2$, $G_{16} = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{17})^2 \times (\mathbb{Z}_{577})^2$, $G_{17} = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{17})^2 \times (\mathbb{Z}_{1733})^2$, and $G_{18} = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_{17})^2 \times (\mathbb{Z}_{3467})^2$ are the only *SP*-groups of this form. ■

We see that the proofs for Propositions 15 and 20 are identical until the later proposition looks at its fourth prime specifically. A proof to show $G \simeq (\mathbb{Z}_{p_1})^2 \times (\mathbb{Z}_{p_2})^2 \times \ldots \times (\mathbb{Z}_{p_n})^2$ is an *SP*-group, where the p_i's are distinct primes with $p_1 < p_2 < \ldots < p_n$ for all $n \in \mathbb{N}$, $n > 3$, would begin the same as the proof for the case with $n-1$ distinct primes. The cases would differ when we try to find what the n^{th} prime would be. We attempt to find this prime knowing $p_n + 1|p_1^2 \cdot p_2^2 \cdots p_{n-1}^2$. We believe that this pattern can be continued

indefinitely, but have not been able to prove our intuition. For example,

$$G = (\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2 \times (\mathbb{Z}_{11})^2 \times (\mathbb{Z}_{17})^2 \times (\mathbb{Z}_{19})^2 \times (\mathbb{Z}_{29})^2 \times (\mathbb{Z}_{37})^2 \times (\mathbb{Z}_{43})^2 \times (\mathbb{Z}_{59})^2$$

is one of many SP-groups using ten distinct prime numbers. To find an eleventh prime, we merely need to find a prime p_{11} so that $p_{11}+1 | 2^2 \cdot 3^2 \cdots 59^2$. One such prime is 67. Unfortunately, there seems to be no pattern as to how we can find these primes short of brute force.

References

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.2; 2000, (`http://www.gap-system.org`).

[1] Pierson, Kenneth, unpublished manuscript; 2001.