A Curious Connection Between Fermat Numbers and Finite Groups

Carrie E. Finch and Lenny Jones

1. INTRODUCTION. In the seventeenth century, Fermat defined the sequence of numbers $F_n = 2^{2^n} + 1$ for $n \geq 0$, now known as *Fermat numbers*. If F_n happens to be prime, F_n is called a *Fermat prime*. Fermat showed that F_n is prime for each $n \leq 4$, and he conjectured that F_n is prime for all n (see Brown [**1**] or Burton [**2**, p. 271]). Almost one hundred years passed before Euler demonstrated in 1732 that F_5 is in fact composite. Ironically, it is now known that F_n is composite for many values of n and, as of the date this article was written, no new Fermat primes had been discovered. In this paper we solve a problem in finite groups whose solution relies heavily on techniques from elementary number theory. While it is not unusual for this phenomenon to occur, the main result is surprisingly a direct consequence of the fact that F_5 is composite.

2. SOME PRELIMINARIES. Throughout this article, G will be a finite abelian group, $|G|$ will denote its cardinality, and $(\mathbb{Z}_m)^t$ will be used to indicate $\underbrace{\mathbb{Z}_m \times \cdots \times \mathbb{Z}_m}_{t \text{ factors}}$.

Definition 1. Let x be an element of G. We define the *order subset* of G determined by x to be the set of all elements in G with the same order as x.

Definition 2. A group G is said to have *perfect order subsets* if the number of elements in each order subset of G is a divisor of $|G|$.

We note that the property of having perfect order subsets is invariant under isomorphism.

Example 1. *Let $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$. Observe that $|G| = 24$. Then G has perfect order subsets, as indicated by the following table:*

Element Order	Cardinality of Order Subset
1	1
2	3
3	2
4	4
6	6
12	8

Since $\mathbb{Z}_3$ has two elements of order 3, it follows that $\mathbb{Z}_3$ does not have perfect order subsets. Consequently, we see from Example 1 that the property of having perfect order subsets is not necessarily passed on to subgroups.

Note that in general, when p is an odd prime, every nonidentity element of $\mathbb{Z}_p$ has order p since, by Lagrange's theorem [**3**, p. 202], the order of any element divides the order of the group. Hence, $\mathbb{Z}_p$ has exactly $p-1$ elements of order p and therefore does not have perfect order subsets. Generalizing further, if C is a cyclic group with $|C|$ a power of an odd prime p, then C contains exactly one subgroup of order p, so C has exactly $p-1$ elements of order p. Thus C does not have perfect order subsets.

Proposition 1. *Suppose that G has perfect order subsets and that p is a prime dividing $|G|$. Then $p-1$ divides $|G|$.*

Proof. To prove this result, we count the number of elements in G of order p. By the Fundamental Theorem of Finite Abelian Groups (see Hungerford [**3**, p. 256]), $G \simeq C_1 \times C_2 \times \cdots \times C_t \times M$, where p does not divide $|M|$ and each C_i is a cyclic group with $|C_i|$ a positive power of p. Each element of G can be thought of as an ordered $(t+1)$-tuple. An element whose order is less than or equal to p must have the identity of M as its entry in the $t+1$ position in the tuple. Each of the other entries must be an element of order at most p in its respective group. Such a tuple will have order exactly p in G, except when the identity appears in each entry. Hence the total number of elements of order p in G is $p^t - 1 = (p-1)(p^{t-1} + p^{t-2} + \cdots + 1)$. Since G has perfect order subsets, the conclusion of the proposition follows. ∎

Corollary 1. *If G has perfect order subsets and is nontrivial, then $|G|$ is even.*

While Proposition 1 imposes severe restrictions on the cardinality of a group with perfect order subsets, it turns out that such groups are, nonetheless, quite plentiful. This fact is formalized in Theorem 1, but some groundwork is needed first.

Lemma 1. *Let a, b, and t be positive integers with $b \leq a$, and let $G \simeq (\mathbb{Z}_{p^a})^t$, where p is a prime. Then the number of elements in G of order p^b is $(p^{b-1})^t(p^t - 1)$.*

Proof. Akin to the proof of Proposition 1, we think of an arbitrary element of G as an ordered t-tuple, where each entry is an element from $\mathbb{Z}_{p^a}$. An element of G whose order is p^b must have an element of order p^b as an entry in at least one of its t positions. To count such elements systematically, we first count the number of tuples with an element of order p^b in the first position, followed by elements of any order less than or equal to p^b in the next $t-1$ positions. The number of elements of order p^b in $\mathbb{Z}_{p^a}$ is the number of generators of the unique cyclic subgroup of $\mathbb{Z}_{p^a}$ of order p^b. This number is $\phi(p^b) = p^b - p^{b-1}$, where ϕ is Euler's totient function [**2**, p. 156]. It determines the number of choices for the first position in the t-tuple. Since we can have any element of $\mathbb{Z}_{p^a}$ with order less than or equal to p^b in the next $t-1$ positions, and there is exactly one subgroup of order p^c for each $c \leq b$ (each having $\phi(p^c)$ generators), there are

$$\begin{aligned} &1 + \phi(p) + \phi(p^2) + \cdots + \phi(p^{b-1}) + \phi(p^b) \\ &\quad = 1 + (p-1) + (p^2 - p) + \cdots + (p^{b-1} - p^{b-2}) + (p^b - p^{b-1}) = p^b \end{aligned}$$

choices for each of those positions. This amounts to

$$\phi(p^b)(p^b)^{t-1}$$

such elements in G.

Next, we count tuples with an element of order strictly less than p^b in the first position, an element of order exactly p^b in the second position, and an element of $\mathbb{Z}_{p^a}$ with order less than or equal to p^b in the next $t-2$ positions. This leads to

$$\begin{aligned}1+\phi(p)+\phi(p^2)+\cdots+\phi(p^{b-1})&\\ =1+(p-1)+(p^2-p)+\cdots+(p^{b-1}-p^{b-2})&=p^{b-1}\end{aligned}$$

choices for the first position, $\phi(p^b)$ choices for the second position, followed by p^b choices for the next $t-2$ position. That is, there are

$$p^{b-1}\phi(p^b)(p^b)^{t-2}$$

such elements in G.

We continue this process, counting elements with entries at the beginning of the tuple having order less than p^b, precisely one entry of order exactly p^b, and then entries of order less than or equal to p^b. Summing the element totals so obtained yields an expression for the total number of elements of order p^b in G:

$$\begin{aligned}&\phi(p^b)(p^b)^{t-1}+p^{b-1}\phi(p^b)(p^b)^{t-2}+\cdots+(p^{b-1})^{t-2}\phi(p^b)p^b+(p^{b-1})^{t-1}\phi(p^b)\\ &\quad=\phi(p^b)(p^{b-1})^{t-1}[p^{t-1}+p^{t-2}+\cdots+p+1]\\ &\quad=p^{b-1}(p-1)(p^{b-1})^{t-1}\left(\frac{p^t-1}{p-1}\right)\\ &\quad=(p^{b-1})^t(p^t-1).\end{aligned}$$

■

Lemma 2. *Let $G\simeq(\mathbb{Z}_{p^a})^t\times M$ and $\hat{G}\simeq(\mathbb{Z}_{p^{a+1}})^t\times M$, where a and t are positive integers and p is a prime that does not divide $|M|$. Suppose that d is the order of an element in $\hat{G}$ and that p^{a+1} does not divide d. Then both G and $\hat{G}$ contain the same number of elements of order d.*

Proof. An arbitrary element of $\hat{G}$ may be represented as an ordered pair (x, y), where x is an element of $(\mathbb{Z}_{p^{a+1}})^t$ and y is an element of M. The order of (x, y) is the least common multiple of the orders of x and y. Since p does not divide $|M|$, this is simply the product of the two orders. Therefore, if d is the order of the element (x, y) and p^{a+1} does not divide d, we can factor d as p^bm, where $0\le b\le a$: p^b is the order of x and m is the order of y. Consequently, to count the number of elements of order p^bm in $\hat{G}$, we count the number of elements in $(\mathbb{Z}_{p^{a+1}})^t$ of order p^b and multiply that quantity by the number of elements of order m in M. By Lemma 1, this total is precisely the same as the number of elements of order p^bm in G. ■

We are now in a position to prove the following.

Theorem 1 (Going-Up Theorem). *Let $G\simeq(\mathbb{Z}_{p^a})^t\times M$ and $\hat{G}\simeq(\mathbb{Z}_{p^{a+1}})^t\times M$, where a and t are positive integers and p is a prime that does not divide $|M|$. If G has perfect order subsets, then $\hat{G}$ has perfect order subsets.*

Proof. As in the proof of Lemma 2, let (x, y) be an element of $\hat{G}$, where x is an element of $(\mathbb{Z}_{p^{a+1}})^t$ and y is an element of M. Let d be the order of (x, y). Assume initially that d is not divisible by p^{a+1}. Since G has perfect order subsets, Lemma 2 guarantees that the cardinality of the order subset of $\hat{G}$ determined by (x, y) divides $|\hat{G}|$.

Suppose next that d is divisible by p^{a+1}. Then the order of x in $(\mathbb{Z}_{p^{a+1}})^t$ is exactly p^{a+1}, and we can factor d as $p^{a+1}m$, where m is the order of y in M. Let k be the number of elements in M that have order m. By Lemma 1, the total number of elements of order d is $(p^a)^t(p^t-1)k$. To complete the proof, we must show that this number does indeed divide $|\hat{G}|$. Applying Lemma 1 to G tells us that the number of elements in G having order $p^a m$ is $(p^{a-1})^t(p^t-1)k$, which divides $|G|$ because G has perfect order subsets. Since $|\hat{G}| = p^t|G|$, it follows that $p^t(p^{a-1})^t(p^t-1)k = (p^a)^t(p-1)k$ divides $|\hat{G}|$. ∎

We give some examples to illustrate Theorem 1.

Example 2. *It is easy to verify that the group* $(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ *has perfect order subsets. The going-up theorem, allowing us to increase the exponent on any of the primes that appear, provides new groups with perfect order subsets. For example,* $(\mathbb{Z}_2)^4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$ *and* $(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$ *also have perfect order subsets. In addition, applying the going-up theorem successively yields groups such as* $(\mathbb{Z}_{16})^4 \times \mathbb{Z}_9 \times \mathbb{Z}_{125}$ *with perfect order subsets.*

The important fact we learn from the going-up theorem is that we can generate new groups with perfect order subsets from existing ones and, by this mechanism, exhibit an infinite number of such groups. This raises a natural question: Is it possible to go the other way? That is, given a "big" group with perfect order subsets, can we develop a technique for finding a "smallest" nontrivial subgroup with perfect order subsets? The answer is yes, and we divide the process for doing so into two steps in order to make the idea more transparent. The details are given in Theorems 2 and 3, but since the proofs are essentially identical, we omit the proof of Theorem 3.

Theorem 2 (Chopping-Off Theorem). *Suppose that* G *has perfect order subsets and that* $G \simeq \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_{s-1}}} \times (\mathbb{Z}_{p^{a_s}})^t \times M$*, where* p *is a prime not dividing* $|M|$ *and* $a_1 \le a_2 \le \cdots \le a_{s-1} < a_s$ *are positive integers. Then* $\hat{G} \simeq (\mathbb{Z}_{p^{a_s}})^t \times M$ *also has perfect order subsets.*

Proof. In this proof, we again think of an element in $\hat{G}$ as an ordered pair (x, y), with x an element of $(\mathbb{Z}_{p^{a_s}})^t$ and y an element of M. As in the proof of Lemma 2, the order of (x, y) can be factored as $p^b m$ with $b \le a_s$, where p^b is the order of x and m is the order of y. Additionally, suppose that $p^c k$, where p does not divide k, is the number of elements in M that have order m. Then, by Lemma 1, the number of elements in $\hat{G}$ that have order $p^b m$ is

$$(p^{b-1})^t(p^t-1)p^c k.$$

We proceed to show that this number is a divisor of $|\hat{G}|$. Again utilizing counting techniques developed in the proofs of Lemma 1 and Lemma 2, we calculate the number of elements in G having order $p^{a_s}m$ to be

$$p^a(p^{a_s-1})^t(p^t-1)p^c k,$$

where $a = \sum_{i=1}^{s-1} a_i$. This number divides $|G|$, for G has perfect order subsets. We conclude that $c \le t$ and that $(p^t-1)k$ is a divisor of $|M|$. Thus, $(p^{b-1})^t(p^t-1)p^c k$ divides $|\hat{G}|$, hence $\hat{G}$ has perfect order subsets. ∎

Theorem 3 (Going-Down Theorem). *Suppose that G has perfect order subsets and that $G \simeq (\mathbb{Z}_{p^a})^t \times M$, where p is a prime not dividing $|M|$. Then $\hat{G} \simeq (\mathbb{Z}_p)^t \times M$ also has perfect order subsets.*

Here is a very simple illustration of the use of these two theorems.

Example 3. *In Example 1, we saw that $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ has perfect order subsets. According to the chopping-off and going-down theorems, $\mathbb{Z}_2 \times \mathbb{Z}_3$ also has perfect order subsets.*

In light of the chopping-off and going-down theorems, given a nontrivial group G with perfect order subsets, we can limit our search for the smallest nontrivial subgroup of G with that property to subgroups H whose Sylow p-subgroups are elementary abelian for each prime p; i.e., each Sylow p-subgroup of H is isomorphic to $(\mathbb{Z}_p)^t$ for some positive integer t. In particular, since a nontrivial group G with perfect order subsets has even order (Corollary 1), there exists a subgroup H of G with perfect order subsets whose Sylow 2-subgroup is elementary abelian. On the basis of these remarks, we formalize the relevant notion of "smallest" in the following definition.

Definition 3. Suppose that $G \simeq (\mathbb{Z}_2)^t \times M$, where $|M|$ is odd. We call G a *minimal POS group* if G has perfect order subsets and there is no proper subgroup $\hat{M}$ of M such that $(\mathbb{Z}_2)^t \times \hat{M}$ has perfect order subsets.

Example 4. *Both $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_2$ have perfect order subsets, but only $\mathbb{Z}_2$ is a minimal POS group.*

3. THE MAIN THEOREM. When $G \simeq (\mathbb{Z}_2)^t \times M$ is a minimal POS group with $|M|$ square-free, the factor M is uniquely determined by the value of t. This is the content of Theorem 4, for which some preliminary remarks might prove useful. Since $(\mathbb{Z}_2)^t$ is a factor of G, there are exactly $2^t - 1$ elements of order 2, and since G has perfect order subsets by the definition of a minimal POS group, $2^t - 1$ must divide $|G|$. Accordingly, G (hence, M) must contain a Sylow p-subgroup for each prime p dividing $2^t - 1$. Thus, we start with a particular value of t, and we attempt to build a minimal POS group by "attaching" cyclic factors to $(\mathbb{Z}_2)^t$ for each of the primes dividing $2^t - 1$. Because a cyclic group whose order is a power of p has exactly $p - 1$ elements of order p, this process is somewhat tricky for the following reason: when we attach a cyclic factor corresponding to a particular prime divisor p of $2^t - 1$, we must then ensure that the prime divisors of $p - 1$ also divide $|G|$; otherwise G would not have perfect order subsets. We might then have to attach even more cyclic factors, which could conceivably produce a factor M whose order is not square-free. In addition, there is no obvious reason why this process of attaching factors should eventually terminate in the desired minimal POS group. It turns out that there are values t for which we can build minimal POS groups, but that there are only finitely many such values. The factors of $2^t - 1$ that, as previously indicated, play a role in the construction of M, are occasionally Fermat numbers. As t grows, we can continue to build minimal POS groups as long as these Fermat numbers are prime. Once we encounter a composite Fermat number, however, the process grinds to a halt. This result is summarized in the following theorem.

Theorem 4. *Let G be a finite abelian group of even order whose Sylow p-subgroup is a cyclic group of order p for each odd prime p dividing $|G|$. If G is a minimal POS group, then G is isomorphic to one of the following nine groups:*

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

The following lemma will be useful in the proof of Theorem 4.

Lemma 3. *Let p be a prime, let a be a positive integer, and let q be a prime divisor of $2^{p^a} - 1$. Then p divides $q - 1$.*

Proof. Since 2^{p^a} is congruent to 1 modulo q, 2^{p^a} represents the identity element in the multiplicative group $(\mathbb{Z}_q)^*$ of nonzero elements of $\mathbb{Z}_q$. It follows that the order of 2 in $(\mathbb{Z}_q)^*$ divides p^a, whence this order is divisible by p. By Lagrange's theorem, the order of an element in a finite group divides the order of the group, and since the order of $(\mathbb{Z}_q)^*$ is $q - 1$, we conclude that p divides $q - 1$. ∎

Proof of Theorem 4. It is straightforward to check that each of the nine indicated groups is, in fact, a minimal POS group. We must verify that the list is exhaustive. Assume that $G \simeq (\mathbb{Z}_2)^t \times M$ is a minimal POS group, where $|M|$ is odd and square-free. There are $2^t - 1$ elements of order 2 in G. Because $2^t - 1$ must therefore divide $|M|$, $2^t - 1$ is square-free. Let p be an odd prime dividing t. Then $2^p - 1$ divides $2^t - 1$ and must also be square-free. If q_1 and q_2 are distinct primes dividing $2^p - 1$ (hence, dividing $|M|$), then p divides both $q_1 - 1$ and $q_2 - 1$ (Lemma 3). Thus p^2 divides $(q_1 - 1)(q_2 - 1)$, the number of elements of order $q_1 q_2$ in G, which by hypothesis divides $|M|$, a contradiction. Hence $2^p - 1$ must be prime. Moreover, since p is odd, we observe that $2^p - 2$ is divisible by 3. If p_1 and p_2 are distinct odd primes dividing t, then 9 divides $(2^{p_1} - 2)(2^{p_2} - 2)$, which is the number of elements of order $(2^{p_1} - 1)(2^{p_2} - 1)$ in G. It follows that 9 divides $|M|$, another contradiction. Hence, at most one odd prime p divides t. Similarly, if $2p$ divides t, where p is an odd prime, then 9 divides $(2^t - 1)(2^p - 2)$, the number of elements in G of order $2(2^p - 1)$. The square-free character of $|M|$ rules out this possibility as well. We infer that t is necessarily a power of a prime.

Suppose next that $t = p^a$, where p is an odd prime and $a \geq 2$. From the foregoing discussion we know that $2^p - 1$ is a prime divisor of $2^{p^a} - 1$. Since $2^{p^a} - 1$ is square-free, it follows that there is some prime $q \neq 2^p - 1$ that divides $2^{p^a} - 1$. From Lemma 1, we conclude that p^2 divides $(q - 1)(2^p - 2)$, the number of elements of order $q(2^p - 1)$ in G , again a contradiction. Hence $t = p^a$ with $a \leq 1$. If $a = 0$, then $t = 1$ and $G \simeq \mathbb{Z}_2$, the first group on our list (remember: G is a minimal POS group). We proceed assuming that $a = 1$, i.e., $t = p$. Since $2(2^{p-1} - 1)$, the number of elements of order $2^p - 1$, divides $|G|$, we can apply the same analysis to the exponent $p - 1$ that we originally applied to t and conclude that $p - 1$ is a power of 2. This makes p a Fermat prime.

To summarize: the preceding arguments show that, except for the trivial case in which $t = 1$ and $G \simeq \mathbb{Z}_2$, either $t = p$, a Fermat prime for which $2^{p-1} - 1$ divides $|G|$, or $t = 2^a$ with $a \geq 1$. In both of the latter instances we are led to a situation where $|G|$

has a factor of the form $2^{2^a} - 1$ with $a \geq 1$. Observe that

$$2^{2^a} - 1 = \prod_{n=0}^{a-1} (2^{2^n} + 1) = \prod_{n=0}^{a-1} F_n,$$

from which it becomes clear that F_5 divides $2^{2^a} - 1$ as soon as $a \geq 6$. However, since 3 divides $2^{2^a} - 1$ and 6700417 is a prime factor of F_5, we see that 9 divides $(2^{2^a} - 1)(6700416)$, the number of elements of order $(2)(6700417)$ in G. Thus 9 divides $|M|$, once more contradicting the fact that $|M|$ is square-free. As a result, $a \leq 5$ and t is a member of $\{2, 3, 4, 5, 8, 16, 17, 32\}$.

By the remarks that prefaced the statement of Theorem 4, any minimal POS group G associated with a given t from the indicated set has a Sylow p-subgroup for each prime p that divides $2^t - 1$. Moreover, $p - 1$ divides $|G|$. Together with the requirement that $|M|$ be square-free, these conditions allow for one and only one group G for each such t, as easy calculations show. This proves that the number of groups of the specified type is finite and, that all groups of this type must appear on the given list. ■

4. CONCLUSION AND OPEN QUESTIONS. This research originated with the observation that S_3, the symmetric group on three letters, has perfect order subsets. Since we first began to explore this phenomenon, our investigations have focused mainly on the abelian case, so the nonabelian case remains somewhat of a mystery. In addition, the only known example of a minimal POS group that contains a noncyclic Sylow p-subgroup of odd order is

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

We conclude with a brief list of open questions.

- Are there nonabelian groups other than S_3 that have perfect order subsets?
- Are there only finitely many minimal POS groups that contain noncyclic Sylow p-subgroups of odd order?
- If G has perfect order subsets and some odd prime p divides $|G|$, then is it true that $|G|$ is divisible by 3?

ACKNOWLEDGEMENT. The authors thank the referee for valuable suggestions.

REFERENCES

1. K. Brown, *Fermat's Fallibility*; retrieved 15 May 2001, from the World Wide Web: http://www.mathpages.com/home/kmath195.htm
2. D. Burton, *Elementary Number Theory*, 2nd ed., Wm. C. Brown Publishers, Dubuque, Iowa, 1989.
3. T. Hungerford, *Abstract Algebra: An Introduction*, 2nd ed., Saunders College Publishing, New York, 1990.

CARRIE E. FINCH received an M.S. degree in theoretical linguistics from Georgetown University in 1998 and an M.S. degree in mathematics from Shippensburg University in 1999. She was an instructor of mathematics at Shippensburg University during the 2000–2001 academic year. She is currently enrolled in a Ph.D. program at the University of South Carolina, where she is studying number theory. Her hobbies include running, playing tennis, swimming, karate, traveling, gourmet dining, and fine wine. By the time this article appears, she will have completed her first marathon.
Department of Mathematics, University of South Carolina, Columbia, SC 29208
cfinch@math.sc.edu

LENNY JONES received his Ph.D. from the University of Virginia in 1987 in representation theory under the supervision of Leonard Scott. He is professor of mathematics at Shippensburg University. His main mathematical interests are in the connections between algebra and number theory. His main nonmathematical interests are traveling, playing music, playing tennis, gourmet dining, and fine wine.
Department of Mathematics and Computer Science, Shippensburg University, Shippensburg, PA 17257
lkjone@ship.edu

A Geometric Telescope

The two most basic series whose sums can be computed explicitly (geometric series, telescoping series) combine forces to demonstrate the amusing fact that

$$\sum_{m=2}^{\infty} (\zeta(m) - 1) = 1,$$

where $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is the Riemann zeta function. Namely,

$$\begin{aligned}\sum_{m=2}^{\infty} (\zeta(m) - 1) &= \sum_{m=2}^{\infty} \sum_{n=2}^{\infty} \frac{1}{n^m} = \sum_{n=2}^{\infty} \sum_{m=2}^{\infty} \left(\frac{1}{n}\right)^m \\ &= \sum_{n=2}^{\infty} \frac{1/n^2}{1 - (1/n)} = \sum_{n=2}^{\infty} \frac{1}{n^2 - n} \\ &= \lim_{N \to \infty} \sum_{n=2}^{N} \left(\frac{1}{n-1} - \frac{1}{n}\right) = \lim_{N \to \infty} \left(1 - \frac{1}{N}\right) = 1 .\end{aligned}$$

Submitted by:
Wg Cdr Thomas Walker
Bangalore, India