Many proofs that the primes are infinite

J. Marshall Ash[†] and T. Kyle Petersen

Theorem 1. *There are infinitely many prime numbers.*

How many proofs do you know that there are infinitely many primes? Nearly every student of mathematics encounters Euclid's classic proof at some point, and many working mathematicians could provide one or two more if asked. If you had to guess, how many different proofs of Theorem 1 do you think there are? A dozen? A hundred?

Certainly many have taken joy in coming up with, and sharing, novel proofs of the theorem. The techniques used have drawn from virtually all parts of mathematics. There have been proofs using the tools of Algebra, Number Theory, Analysis, and even Topology![1]

Our goal here is not to catalogue or classify the proofs that have appeared in the literature. Rather, we propose the following as exercise to enhance a number theory class, a history of math class, a senior capstone class, a math club meeting, et cetera:

Exercise 1. *Pick a known proof of the infinitude of the primes and expand it into an* infinite family of proofs.

We shall give several examples below. Our first one converts a well known modernization of Euclid's 2300 year old proof of Theorem 1 into an infinite number of similar, but distinct, proofs.

Example 1. Assume that the number of primes is finite, and label them $p_1, \dots, p_n$. Let k be any positive integer. Here is the kth proof: Form

$$N = N(k) = k \cdot p_1 \cdots p_n + 1.$$

On the one hand, division of N by any prime leaves a remainder of 1, while on the other hand, N being an integer greater than 1 means that N has a prime factor q and division of N by the prime q leaves a remainder of 0. This contradiction means that the number of primes is infinite. □

Thus, for each positive integer k, we have a different proof of Theorem 1. Our next proof is modeled on a classical analytical argument, usually attributed to Euler.

We begin with Euler's wonderful formula

$$\prod_{p \text{ is prime}} \frac{1}{1-\frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{0.1}$$

Both sides are infinite if $s \in (0,1]$; when $s > 1$, the right side is called $\zeta(s)$. This is known to be a rational multiple of π^s when s is a positive even integer. For some discussion of the history of this formula in relation to the infinitude of the primes, see [**Co**].

[†] Research partially supported by DePaul University Faculty Summer Research Grants.

[1] To get some idea for this variety, there are several good resources. The webpage [**Ca**] contains five proofs, the book [**AZ**] contains six, and the book [**R**] has eleven. Another source is pages 413–415 of [**D**].

Example 2. Assume that the set of primes has finite cardinality. Let k be any positive integer. Here is the kth proof: Let $s = 2k$. The left hand side of Equation (0.1) is a finite product of rational numbers and hence is rational. But because π is transcendental, π^{2k} is irrational, and hence the right hand side of Equation (0.1) is irrational. This is a contradiction. □

Our first two examples have clearly established the following.

Theorem 2. *The set of proofs of Theorem 1 is infinite.*

So far we have only seen that there are *countably* many proofs that there are infinitely many primes. Can we do better? The answer is yes, we can produce an uncountable family of proofs of Theorem 1, as the next example shows. We use Euler's formula (0.1) again, this time with the parameter s being any real number with $0 < s \leq 1$.

Example 3. Again assume that the set of primes has finite cardinality. Fix s, an arbitrary real number such that $0 < s \leq 1$. Here is the sth proof: The left hand side of Equation (0.1) is a finite product of real numbers and hence is the finite real number

$$L = L(s) = \left(\frac{1}{1-\frac{1}{2^s}}\right)\left(\frac{1}{1-\frac{1}{3^s}}\right)\cdots\left(\frac{1}{1-\frac{1}{P^s}}\right),$$

where P is the last prime. Expanding each term as a geometric series gives

$$L = \left(1+\tfrac{1}{2^s}+\left(\tfrac{1}{2^s}\right)^2+\cdots\right)\left(1+\tfrac{1}{3^s}+\left(\tfrac{1}{3^s}\right)^2+\cdots\right)\cdots\left(1+\tfrac{1}{P^s}+\left(\tfrac{1}{P^s}\right)^2+\cdots\right).$$

If $n = 2^a 3^b \cdots P^z$ is an arbitrary positive integer, multiplying together the $a+1$th term of the first factor, the $b+1$th term of the second factor, ..., and the $z+1$th term of the last factor shows that the expansion of L contains the term $\frac{1}{n^s}$. It follows that no matter how large k might be,

$$\begin{aligned}
L &> 1+\frac{1}{2^s}+\left(\frac{1}{3^s}+\frac{1}{4^s}\right)+\cdots+\left(\frac{1}{\left(2^{k-1}+1\right)^s}+\cdots+\frac{1}{\left(2^k\right)^s}\right)\\
&> 1+\frac{1}{2^s}+\left(\frac{1}{4^s}+\frac{1}{4^s}\right)+\cdots+\left(\frac{1}{\left(2^k\right)^s}+\cdots+\frac{1}{\left(2^k\right)^s}\right)\\
&= 1+\frac{1}{2}2^{1-s}+\frac{1}{2}\left(2^{1-s}\right)^2+\cdots+\frac{1}{2}\left(2^{1-s}\right)^k\\
&\geq 1+\frac{k}{2}.
\end{aligned}$$

The final inequality follows since $1-s \geq 0$ and so $2^{(1-s)} \geq 1$. But this is impossible since L is fixed and k can be chosen arbitrarily large. □

One can even stretch the size of this family of proofs from the cardinality of the continuum, $\mathfrak{c}$, to $2^{\mathfrak{c}}$ by beginning "Fix S, an arbitrary nonempty subset of $(0,1]$. Here is the Sth proof..." and then proceeding with substantially the same proof. Below is a controversial example of a family of proofs of arbitrarily large cardinality.

Example 1 on steroids. Let S be any (very large) set and let f be a function from S to the positive integers. Assume that the number of primes is finite, and label them $p_1, \ldots, p_n$. Let α be any element of S. Here is the αth proof: Let

$$N = N(\alpha) = f(\alpha)\cdot p_1\cdots p_n + 1.$$

As in the opening example, N both does and does not have a prime factor. □

Formally we have presented as many proofs as the cardinality of the arbitrarily chosen set S. When S is uncountable, this family of proofs will only be acceptable to a reader who is willing to agree that proof α is distinct from proof β when $f(\alpha) = f(\beta)$.

Our last example will show how a single proof can easily lead to a variety of different proof families. Further, it gives an elementary example of an uncountable family of proofs. The basic proof on which these are built is due to [**S**].

Example 4a. Choose any integer $n > 1$. Here is the nth proof: Clearly, $\gcd(n, n+1) = 1$, so the product $n_1 = n(n+1)$ has at least two distinct prime factors. Now recursively define $n_r = n_{r-1}(n_{r-1}+1)$ for any $r > 1$. Since $\gcd(n_{r-1}, n_{r-1}+1) = 1$, we know n_r has at least one more prime factor than n_{r-1} has. As n_1 has at least two distinct prime factors, we can conclude that n_r has at least $r+1$ distinct prime factors. Thus, the number of primes is unbounded. □

Example 4b. Now, when we choose $n > 1$, we also choose an integer $k \geq 1$. Here is proof (n, k): Let $n_1 = kn(n+1)$. The factor of k does not prevent us from concluding, as before, that n_1 has at least two distinct prime factors. Recursively, we conclude that $n_r = kn_{r-1}(n_{r-1}+1)$ has at least $r+1$ distinct prime factors. □

Example 4c. Along with n and k, choose an integer $l \geq 1$. For proof (n, k, l), we observe that $\gcd(n, ln+1) = 1$ and so $n_1 = kn(ln+1)$ has at least two distinct prime factors. Recursively, $n_r = kn_{r-1}(ln_{r-1}+1)$ has at least $r+1$ distinct prime factors. □

Example 4d. Choose n and k as before, but instead of l take f to be any non-constant polynomial with nonnegative integer coefficients and constant term 1, e.g., $3x^5 + 2x^2 + 1$. (The nonnegative restriction isn't strictly necessary, but we don't want to have the polynomial evaluate to 1 at any point.) Here is proof (n, k, f): For any integer $n > 1$, we have $\gcd(n, f(n)) = 1$. So (with $n = n_0$) define recursively $n_r = kn_{r-1}f(n_{r-1})$. The conclusions are the same. □

Example 4e. Now choose n, a sequence of positive integers: $k_1, k_2, \ldots$, and a sequence of non-constant polynomials with nonnegative integer coefficients and constant term 1: $f_1, f_2, \ldots$. For proof $(n, k_1, k_2, \ldots, f_1, f_2, \ldots)$, we now define $n_r = k_r n_{r-1} f_r(n_{r-1})$, and the conclusion is the same. □

As the set of all sequences of positive integers is uncountable (as is the set of sequences of polynomials described) the family of Example 4e is a continuum.

Final remarks. We welcome the reader to construct his or her own family of proofs, and to compare and contrast that family with the different families of proof given here. As a discussion point, we invite the reader to ask: How new are these proofs, *really*? What makes one proof distinct from another? Certainly, a proof taken from Example 1 is distinct from a proof given in Example 2. But within a family, how different is proof k from proof $k+1$?

Finally, we wish to mention a paper of L. P. J. Kilford [**K**] that gives the first example of a solution to our proposed exercise. Though we were not aware of this work before writing the present article, its publication certainly preceded the first draft of this article. Thanks to Roger Cooke for calling it to our attention.

References

[AZ] M. Aigner and G. M. Ziegler, *Proofs from the book*, Springer

[Ca] C. K. Caldwell, Proofs that there are infinitely many primes, available online at: `http://primes.utm.edu/notes/proofs/infinite/`

[Co] R. Cooke, Life on the mathematical frontier: legendary figures and their adventures, Notices of the Amer. Math. Soc., **57**(2010), 464–475.

[D] L. E. Dickson, *History of the Theory of Numbers, volume 1: Divisibility and Primality,* Carnegie Institute of Washington, Washington, DC, 1919.

[K] L. J. P. Kilford, An infinitude of proofs of the infinitude of primes, `http://arxiv.org/abs/math/0610066`, 2008.

[R] P. Ribenboim, *The new book of prime number records*, Springer, 1995

[S] F. Saidak, A new proof of Euclid's theorem, Amer. Math. Monthly, **113**(2006), 937–938.

Mathematics Department, DePaul University, Chicago, IL 60614
E-mail address: mash@math.depaul.edu
URL: http://math.depaul.edu/~mash/

Mathematics Department, DePaul University, Chicago, IL 60614
E-mail address: tkpeters@math.depaul.edu
URL: http://math.depaul.edu/~tpeter21/