YET ANOTHER PROOF OF THE INFINITUDE OF PRIMES, I

MICHAEL COONS

Any good theorem should have several proofs, the more the better.
—Sir Michael Atiyah [2, Page 223]

The following well–known result can be found in Book IX (Proposition 20) of Euclid's *Elements*. The proof given here is G. H. Hardy's taken (nearly verbatim) from *A Mathematician's Apology* [1, Page 93], which is very similar to Euclid's original proof.

Euclid's Theorem. *There are infinitely many primes.*

Hardy's proof of Euclid's Theorem. Let us suppose that the number of primes is finite, and that

$$2, 3, 5, \ldots, P$$

is the complete series (so that P is the largest prime); and let us, on this hypothesis, consider the number Q defined by the formula

$$Q = (2 \cdot 3 \cdot 5 \cdots P) + 1.$$

It is plain that Q is not divisible by any of $2, 3, 5, \ldots, P$; for it leaves a remainder 1 when divided by any of these numbers. But Q must be divisible by one of $2, 3, 5, \ldots, P$ since these are all the primes, which gives us a contradiction. □

Euclid's proof (reflected above in a modernization given by Hardy) is surely one of the most elegant arguments in mathematics, and to use a phrase from Erdős, very well may be a "proof from the book." The proof is easily digested and leaves nothing in question about the fact that there are indeed infinitely many primes. The above proof demonstrates that a finite number of primes is not enough, but this leads us to ask the question: *how many numbers can one make with a finite number of primes?*

To answer this question a little more thoroughly, we offer an alternative proof of Euclid's result. But first some notation and a lemma.

Let $N_n(a_1, \ldots, a_n; x)$ represent the number of n–tuples $(k_1, \ldots, k_n)$ such that $a_1^{k_1} \cdots a_n^{k_n} \leq x$. The following lemma should be readily apparent, but we have added the proof for completeness.

Lemma. *Let $a_1, a_2, \ldots, a_n$ be positive integers. Then for any $x > 0$ we have*

$$N_n(a_1, \ldots, a_n; x) \leq N_{n-1}(a_1, \ldots, a_{n-1}; x) \cdot N_1(a_n; x). \tag{1}$$

Date: January 12, 2010.
The research of M. Coons is supported by a Fields–Ontario Fellowship.

Proof. The sum on the left–hand side of (1) is equal to the size of the set

$$A := \{m \le x : m = a_1^{k_1} \cdots a_n^{k_n} \text{ for some } k_1, \ldots, k_n \ge 0\},$$

and the product of sums on the right–hand side of (1) is equal to the size of the set

$$B := \{m : m = a_1^{k_1} \cdots a_n^{k_n} \text{ for some } k_1, \ldots, k_n \ge 0 \\ \text{where both } a_1^{k_1} \cdots a_{n-1}^{k_{n-1}} \le x \text{ and } a_n^{k_n} \le x\}.$$

Thus to prove the lemma, we need to show that the number of elements in A is at most the number of elements in B. Since both A and B are finite sets, it is enough to show that $A \subseteq B$.

To this end, let $m \in A$. Then there exist $k_1, \ldots, k_n \ge 0$ for which

$$m = a_1^{k_1} \cdots a_n^{k_n} \le x.$$

Note that also $m = a_1^{k_1} \cdots a_{n-1}^{k_{n-1}} \cdot a_n^{k_n}$, and that since $m \le x$, we have both

$$a_{n-1}^{k_{n-1}} \le \frac{x}{a_n^{k_n}} \le x$$

and

$$a_n^{k_n} \le \frac{x}{a_1^{k_1} \cdots a_{n-1}^{k_{n-1}}} \le x.$$

Thus $m \in B$, so that $A \subseteq B$ and the lemma is proved. □

Our proof of Euclid's Theorem. Let $p_1, p_2, \ldots, p_n$ be distinct primes and consider

$$N_n(p_1, \ldots, p_n; x).$$

By applying the lemma exactly $n-1$ times we have

$$N_n(p_1, \ldots, p_n; x) \le N_1(p_1; x) \cdot N_1(p_2; x) \cdots N_1(p_n; x).$$

For $i = 1, 2, \ldots, n$, we have that $p_i \ge 2$ so that $\log p_i \ge \log 2$. Thus

$$N_1(p_i; x) \le \frac{\log x}{\log p_i} + 1 \le \frac{\log x}{\log 2} + 1.$$

Putting this together gives for $x \ge e$ that

$$N_n(p_1, \ldots, p_n; x) \le \left(\frac{\log x}{\log 2} + 1\right)^n \le \left(\frac{2}{\log 2}\right)^n \log^n x. \tag{2}$$

If there were finitely many primes, say n, then since there are no less than $x-1$ positive integers less than x, we would have to have

$$x - 1 \le N_n(p_1, \ldots, p_n; x)$$

gives for all $x \ge e$ that

$$0 \le \left(\frac{2}{\log 2}\right)^n \log^n x - x + 1, \tag{3}$$

which cannot happen for x large enough. We can use first–year calculus to show this; we need only that eventually the inequality (3) fails. To this end, note that

$$\lim_{x\to\infty} \frac{d}{dx}\left\{\left(\frac{2}{\log 2}\right)^n \log^n x - x + 1\right\} \\ = \lim_{x\to\infty}\left\{(n-1)\left(\frac{2}{\log 2}\right)^n \frac{\log^{n-1} x}{x} - 1\right\} = -1, \tag{4}$$

since for any integer k we have $\lim_{x\to\infty} \frac{\log^k x}{x} = 0$.

Thus eventually (3) fails and we have a contradiction, and so there must be infinitely many primes. □

Our proof is certainly longer than Euclid's and many others (see [3, Chap. 1] for a collection of short proofs), though we think it has merit in other ways. For example, it teaches a student to count a little, and it is appropriate for a first–year calculus course.

Remark. We note here that our proof bears similarities to that of Auric from 1915. See Ribenboim [3, Page 9] for the details of Auric's proof.

References

1. G. H. Hardy, *A mathematician's apology*, Canto, Cambridge University Press, Cambridge, 1992, With a foreword by C. P. Snow, Reprint of the 1967 edition.
2. Martin Raussen and Christian Skau, *Interview with Michael Atiyah and Isadore Singer*, Notices Amer. Math. Soc. **52** (2005), no. 2, 225–233.
3. Paulo Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1996.

University of Waterloo, Dept. of Pure Mathematics, Waterloo, Ontario, N2L 3G1
E-mail address: mcoons@math.uwaterloo.ca