AN IRRATIONAL PROOF THAT THERE ARE INFINITELY MANY RATIONAL PRIMES

PAUL POLLACK

Abstract. We present another proof that there are infinitely many primes, based on the result that $\sqrt{m}$ is irrational whenever the natural number m is not a perfect square.

1. Introduction

In his *Mathematician's Apology* [2, §§12–13], Hardy singles out two results of the ancient Greeks as "theorems of the highest class": the infinitude of the primes and the irrationality of $\sqrt{2}$. The purpose of this note is to forge a connection between these two results. Specifically, we will argue that the infinitude of the primes is a simple consequence of the following theorem:

Theorem A. *If m is a natural number, then $\sqrt{m}$ is rational only when m is a perfect square.*

In order to keep the exposition as elementary as possible, we assume as little number theory as possible. We do use the result that every natural number can be written as a (possibly empty) product of primes, which is an easy exercise in induction, but we have no need for the fundamental theorem of arithmetic, asserting that all such decompositions are unique. One should note that while Theorem A is often presented as a consequence of this fundamental theorem, such a powerful tool is by no means necessary. A very short number theory-free proof of Theorem A is presented in [1, Proposition 1].

2. Proof

Say that a set of natural numbers S has the *twin property* if for some natural number d, there are infinitely many $n \in S$ for which both n and $n + d$ belong to S. We need the following simple lemma:

Lemma. *Let r be a natural number. Suppose that $S_1, \dots, S_r$ are subsets of $\mathbf{N}$ and that $\cup_{i=1}^{r} S_i$ contains all but at most finitely many natural numbers. Then at least one S_i has the twin property.*

Proof. If S is a set of natural numbers, we write $S(N)$ for the number of elements of S not exceeding N. We claim that if S does not have the twin property, then $S(N)/N \to 0$ as $N \to \infty$. This is clear for finite sets S. If S is infinite, list the elements of S, say $n_1 < n_2 < n_3 < \dots$, and for each $i \geq 1$, put $d_i := n_{i+1} - n_i$. Our hypothesis implies that d_i assumes any given value at most finitely many

1991 *Mathematics Subject Classification.* 11A41.
The author is supported by NSF award DMS-0802970.

times. As a consequence, for each $B > 0$, there is a natural number i_0 with the property that $d_i > B$ whenever $i \geq i_0$. For each large N, list the elements $n_1 < n_2 < \cdots < n_k \leq N$, so that $k = S(N)$. Then we have

$$N \geq n_k \geq n_k - n_{i_0} = \sum_{j=i_0}^{k-1} d_j \geq B(k - i_0).$$

Hence $S(N) = k \leq N/B + i_0$, and so $\limsup_{N\to\infty} S(N)/N \leq B^{-1}$. Since B was arbitrary, $S(N)/N \to 0$, as claimed.

So if no S_i has the twin property, then $S_i(N)/N \to 0$ for each $1 \leq i \leq r$, and so $\frac{1}{N}\sum_{i=1}^{r} S_i(N) \to 0$. But this is incompatible with the estimate

$$\sum_{i=1}^{r} S_i(N) \geq \#\left((\cup_{i=1}^{r} S_i) \cap [1, N]\right) \geq N - t \quad \text{for all natural numbers } N,$$

where $t := \#(\mathbf{N} \setminus \cup_{i=1}^{r} S_i)$. □

Say that a number $n \in \mathbf{N}$ is *squarefree* if n is not divisible by the square of an integer larger than 1. Notice that each such n can be written as a product of distinct primes. (The converse, that any product of distinct primes is squarefree, lies slightly deeper and is not needed in the sequel.)

For each $m \in \mathbf{N}$, let v be the largest natural number for which v^2 divides m, and write $m = uv^2$. Then necessarily u is squarefree; we call u the *squarefree part* of m.

Proof that there are infinitely many primes. Suppose that there are only finitely many primes. Then there are only finitely many products of distinct primes, and so *a fortiori*, only finitely many squarefree numbers. For each natural number $n > 1$, write

$$n^2 - 1 = u_n v_n^2,$$

where u_n is the squarefree part of $n^2 - 1$. By hypothesis, u_n assumes only finitely many values, and so if we partition according to the value of u_n, we obtain a finite partition of $\mathbf{N} \setminus \{1\}$. So by the lemma, for some fixed squarefree number u, the set

$$S := \{n \in \mathbf{N} : n^2 - 1 \text{ has squarefree part } u\} \tag{1}$$

has the twin property. That is, for a certain fixed $d \in \mathbf{N}$, there are infinitely many elements $n \in S$ for which $n' := n + d$ also belongs to S. From

$$n^2 - 1 = u \cdot v_n^2 \quad \text{and} \quad n'^2 - 1 = u \cdot v_{n'}^2$$

we deduce that

$$\begin{aligned}(v_{n'} - v_n)\sqrt{u} &= \sqrt{u \cdot v_{n'}^2} - \sqrt{u \cdot v_n^2} \\ &= \sqrt{n'^2 - 1} - \sqrt{n^2 - 1}.\end{aligned}$$

As $n \to \infty$, this last expression converges to d, because $n' - n = d$ while

$$n - \frac{1}{n} \leq \sqrt{n^2 - 1} < n \quad \text{and} \quad n' - \frac{1}{n'} \leq \sqrt{n'^2 - 1} < n'.$$

So $v_{n'} - v_n$ must converge to $d/\sqrt{u}$. Since each difference $v_{n'} - v_n$ is a natural number, it must be that $d/\sqrt{u} = e$ for some natural number e. But then $d/e = \sqrt{u}$, and so $\sqrt{u}$ is rational.

So by Theorem A, u is a perfect square. Since u is squarefree, $u = 1$. But u_n is never equal to 1, as one sees by rewriting the equation $n^2 - 1 = v^2$ in the form $(n - v)(n + v) = 1$. So the set of n with $u_n = 1$ certainly does not have the twin property. □

3. Theorem A: An irrational hypothesis?

What does it mean for the proof of one theorem to rely on another? This seems somewhat ill-defined. Our proof of the infinitude of the primes, as presented above, certainly appears to depend on Theorem A. But actually Theorem A can be dispensed with, as pointed out to the author by Carl Pomerance: Indeed, suppose (as above) that for a certain fixed $d \in \mathbf{N}$, there are infinitely many natural numbers $n \in S$ with $n' := n + d \in S$. We have

$$v_{n'} - v_n = \frac{\sqrt{(n+d)^2 - 1} - \sqrt{n^2 - 1}}{\sqrt{u}}. \tag{2}$$

The right-hand side of (2) is bounded as a function of n, and so we can pass to an infinite subsequence on which $v_{n'} - v_n$ is constant. But this is absurd, since it is a straightforward exercise in calculus to show that the right-hand side of (2) is strictly decreasing for natural numbers n.

4. A variant argument and some concluding remarks

If we are content to use a little bit more number theory, we can give a much shorter argument in the same spirit as that presented in §2: Let $u > 1$ be a fixed squarefree number. If n and v are natural numbers with $n^2 - 1 = uv^2$, then $(n - v\sqrt{u})(n + v\sqrt{u}) = 1$. Since also $n > v\sqrt{u}$, we have

$$\left|\frac{n}{v} - \sqrt{u}\right| = \frac{1}{v}|n - v\sqrt{u}| = \frac{1}{v(n + v\sqrt{u})} \leq \frac{1}{2\sqrt{u}}\frac{1}{v^2} < \frac{1}{2v^2}.$$

This inequality implies (by a well-known theorem of Legendre [3, Theorem 184]) that $n = P_m$ and $v = Q_m$ for some convergent P_m/Q_m in the continued fraction expansion of $\sqrt{u}$. But P_m and Q_m satisfy recurrence relations which guarantee that each of them grows at least exponentially (see [3, Theorem 149]). Consequently, if we define S by (1), then $S(N)/N \to 0$. Since we cannot write the set of natural numbers $n > 1$ as a finite union of sets S where $S(N)/N \to 0$, it follows that there must be infinitely many squarefree numbers u, and so also infinitely many primes.

This argument has the advantage of being related to some deep results in the theory of Diophantine approximation. Indeed, suppose we replace the exponent "2" by "3" in the above. Thus, for each $n > 1$, we now write $n^3 - 1 = uv^3$, where u and v and natural numbers and u is assumed to be *cube*-free. As before, we must have $u > 1$. Moreover,

$$\left|\frac{n}{v} - \sqrt[3]{u}\right| \leq \frac{1}{3v^3u^{2/3}} < \frac{1}{v^3}. \tag{3}$$

Thus n/v must be an extraordinarily good rational approximation to $\sqrt[3]{u}$. In fact, by a theorem of Thue from 1909, only finitely many rational numbers n/v can satisfy (3). This result of Thue was the first nontrivial step towards a deep theorem of Roth, for which he was awarded the Fields Medal in 1958: *If α is an irrational algebraic number, then $|p/q - \alpha| > c(\alpha, \epsilon)/q^{2+\epsilon}$ for each $\epsilon > 0$ and each rational number p/q.*

It follows that if we let S be the set of natural numbers $n > 1$ for which $n^3 - 1$ has a fixed cube-free part u, then S is finite for every choice of u. This has the following interesting consequence, which strengthens the assertion that there are infinitely many primes:

Theorem. *As n tends to infinity, the largest prime factor of $n^3 - 1$ also tends to infinity.*

The proof is immediate from the preceding remarks and the observation that for any bound B, there are only finitely many cube-free numbers all of whose prime factors are bounded by B. In fact, it can be shown that if f is an integer-valued polynomial, then the largest prime factor of $f(n)$ tends to infinity precisely when f has at least two distinct complex roots (see the references of [4, §IV.12]).

Acknowledgements

My thanks go out to Mits Kobayashi, Carl Pomerance, Vicki Reuter, and Enrique Treviño for comments that helped to improve the accuracy and readability of this note.

References

1. R. Beigel, *Irrationality without number theory*, Amer. Math. Monthly **98** (1991), no. 4, 332–335.
2. 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.
3. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman.
4. J. Sándor, D. S. Mitrinović, and B. Crstici, *Handbook of number theory. I*, Springer, Dordrecht, 2006, Second printing of the 1996 original.

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, Urbana, IL 61801
E-mail address: pppollac@illinois.edu