Different ways to prove there are infinitely many primes?

This is just a curiosity. I have come across multiple proofs of the fact that there are infinitely many primes, some of them were quite trivial, but some others were really, really fancy. I'll show you what proofs I have and I'd like to know more because I think it's cool to see that something can be proved in so many different ways.

Proof 1 : Euclid's. If there are finitely many primes then $p_1 p_2 \dots p_n + 1$ is coprime to all of these guys. This is the basic idea in most proofs : generate a number coprime to all previous primes.

Proof 2 : Consider the sequence $a_n = 2^{2^n} + 1$. We have that

$$2^{2^n} - 1 = (2^{2^1} - 1) \prod_{m=1}^{n-1} (2^{2^m} + 1),$$

so that for $m < n$, $(2^{2^m} + 1, 2^{2^n} + 1) \mid (2^{2^n} - 1, 2^{2^n} + 1) = 1$. Since we have an infinite sequence of numbers coprime in pairs, at least one prime number must divide each one of them and they are all distinct primes, thus giving an infinity of them.

Proof 3 : (Note : I particularly like this one.) Define a topology on $\mathbb{Z}$ in the following way : a set $\mathscr{N}$ of integers is said to be open if for every $n \in \mathscr{N}$ there is an arithmetic progression $\mathscr{A}$ such that $n \in \mathscr{A} \subseteq \mathscr{N}$. This can easily be proven to define a topology on $\mathbb{Z}$. Note that under this topology arithmetic progressions are open and closed. Supposing there are finitely many primes, notice that this means that the set

$$\mathscr{U} \overset{def}{=} \bigcup_p p\mathbb{Z}$$

should be open and closed, but by the fundamental theorem of arithmetic, its complement in $\mathbb{Z}$ is the set $\{-1, 1\}$, which is not open, thus giving a contradiction.

Proof 4 : Let a, b be coprime integers and $c > 0$. There exists x such that $(a + bx, c) = 1$. To see this, choose x such that $a + bx \not\equiv 0 \bmod p_i$ for all primes p_i dividing c. If $a \equiv 0 \bmod p_i$, since a and b are coprime, b has an inverse mod p_i, call it $\overline{b}$. Choosing $x \equiv \overline{b} \bmod p_i$, you are done. If $a \not\equiv 0 \bmod p_i$, then choosing $x \equiv 0 \bmod p_i$ works fine. Find x using the Chinese Remainder Theorem.

Now assuming there are finitely many primes, let c be the product of all of them. Our construction generates an integer coprime to c, giving a contradiction to the fundamental theorem of arithmetic.

Proof 5 : Dirichlet's theorem on arithmetic progressions (just so that you not bring it up as an example...)

Do you have any other nice proofs?

(number-theory) (prime-numbers) (big-list)

edited Jul 7 '11 at 5:07

community wiki
3 revs, 2 users 100%
Patrick Da Silva

protected by Asaf Karagila Aug 8 '15 at 21:48

This question is protected to prevent "thanks!", "me too!", or spam answers by new users. To answer it, you must have earned at least 10 reputation on this site (the association bonus does not count).

3 This should be community wiki. Anyway, here's one: the harmonic series diverges, so by considering the Euler product, there must be infinitely many primes. A bit of a sledgehammer though... – Zhen Lin Jul 7 '11 at 4:41

5 That first proof is Euclid's, not Euler's. – Gerry Myerson Jul 7 '11 at 4:42

10 Chapter 1 of Aigner-Ziegler, *Proofs from THE BOOK* contains six proofs (most of them were already mentioned, though). – t.b. Jul 7 '11 at 5:02

9 @Patrick: it is strange that, having asked for proofS, you accepted one answer... – Mariano Suárez-Álvarez ♦ Jul 7 '11 at 5:09

4 Euclid's proof is misrepresented here, as it is by many illustrious authors. Euclid never assumed there are only finitely many; his proof was not by contradiction Catherine Woodgold and I published a paper about this misunderstanding: "Prime Simplicity", *Mathematical Intelligencer*, Volume 31, Number 4, 44-52, DOI: 10.1007/s00283-009-9064-8 – Michael Hardy Nov 17 '11 at 1:13

|

20 Answers

When I taught undergraduate number theory I subjected my students to a barrage of proofs of the infinitude of the prime numbers: see these lecture notes. I gave eight proofs altogether. Of course by now the list which has been currently compiled has a large overlap with mine, but one proof which has not yet been mentioned is Washington's algebraic number theory proof:

Proposition: Let R be a Dedekind domain with fraction field K. If R has only finitely many

prime ideals, then for every finite degree field extension L/K, the integral closure S of R in L is a PID.

(The proof boils down to two facts: (i) a Dedekind domain with finitely many prime ideals is a PID. (ii) with notation as above, the map Spec S $\to$ Spec R is surjective and at most $[L:K]$-to-one, so R has infinitely many prime ideals iff S has infinitely many prime ideals.)

Corollary: There are infinitely many primes.

Proof: Applying the Proposition with $R = \mathbb{Z}$, if there were only finitely many primes, then for every number field K, the ring $\mathbb{Z}_K$ of integers in K would be a PID, hence a UFD. But for instance this fails for $K = \mathbb{Q}(\sqrt{-5})$, as $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ is a nonunique factorization into ireducible elements (since there are no elements of norm 2 or 3) in $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$.

answered Jul 7 '11 at 6:53 — community wiki — Pete L. Clark

+1 I like this argument! – Amitesh Datta Jul 7 '11 at 12:12

I must admit I don't know anything about algebraic number theory to understand your argument, but I'll be taking a course this year about that so I guess I'll read it later on. =) +1 – Patrick Da Silva Jul 7 '11 at 20:17

1 By the way, maybe I should say that I didn't give all eight proofs in my lectures (or maybe I shouldn't, so that people will think that I cover everything in my classes that appears in my lecture notes: that would be pretty impressive). This proof I either skip entirely or summarize as "Actually, it is possible to deduce the infinitude of the prime numbers directly from the lack of unique factorization in $\mathbb{Z}[\sqrt{-5}]$, but this requires methods from more advanced number theory." – Pete L. Clark Jul 7 '11 at 20:40

@Pete L. Clark : Now that I understand your proof, I am amazed by the fact that 5 actually allows you to finish this argument! I know there are other examples, but in the other proofs we never had to consider any particular prime, which is the case in this proof, because "you need" a counter example. This seems to be a general techinque to prove that $|\mathrm{Spec}(R)| = \infty$ in other rings than $\mathbb{Z}$ though... – Patrick Da Silva Oct 26 '13 at 1:14

The following proof is morally due to Euler. We have

$$\prod_{p \text{ prime}} \left(\frac{1}{1 - \frac{1}{p^2}} \right) = \zeta(2) = \frac{\pi^2}{6}.$$

The RHS is irrational, so the LHS must have infinitely many factors.

answered Jul 7 '11 at 4:52 — community wiki — Qiaochu Yuan

8 One can write down the same proof with Apéry's theorem and $\zeta(3)$, but that is *really* overkill... – Qiaochu Yuan Jul 7 '11 at 5:17

3 I wonder what the fact that $\frac{\pi^2}{6}$ is transcendental tells us about the distribution of prime numbers. – Baby Dragon Jun 7 '13 at 3:13

But the formula is derived after knowing there are infinite primes right? So this proof is circular. – N.S.JOHN Apr 28 '16 at 3:07

@N.S.JOHN: no, you don't need to know anything about how many primes there are to prove this formula. – Qiaochu Yuan Apr 28 '16 at 3:08

Alright then .. – N.S.JOHN Apr 28 '16 at 3:10

The following proof is due to Euler. We have

$$\prod_{p \text{ prime}, p \leq m} \left(\frac{1}{1 - \frac{1}{p}} \right) \geq \sum_{n=1}^{m} \frac{1}{n}.$$

The RHS diverges as $m \to \infty$, so the LHS must have an unbounded number of factors.

edited Jul 7 '11 at 4:52 — community wiki — 2 revs — Qiaochu Yuan

Didn't think of the ones with Euler products, I never came across those. Thanks for both proofs! – Patrick Da Silva Jul 7 '11 at 5:00

@Patrick: well, this is just a simplified version of an argument about the zeta function, and such arguments are of course the heart of the proof of Dirichlet's theorem. – Qiaochu Yuan Jul 7 '11 at 5:11

let $p_1, \ldots, p_n$ be the primes less or equal N. any integer less or equal N can be written as

$p_1^{e_1} \cdot \ldots \cdot p_n^{e_n} \cdot m^2$ with $e_i \in \{0,1\}$ and $m \leq \sqrt{N}$. so there are at most $2^n\sqrt{N}$ integers less or equal N, i.e. $N \leq 2^n\sqrt{N}$. simplifying and taking logarithms gives $(1/2)\log N \leq n \log 2$ since N is unbounded, so is n. (due to erdos taken from the book "gamma" by julian havil, a book on euler's constant)

answered Jul 7 '11 at 13:31 — community wiki — yoyo

1 I don't remember seeing this proof. I like it a lot. – Geoff Robinson Jul 7 '11 at 17:18

1 Yes, it's quite nice. It can be extracted from the sixth proof in *Proofs from the Book*, which is also attributed to Erdős. It is a stronger version of the counting proof I gave and gives a slightly stronger "weak PNT." – Qiaochu Yuan Jul 7 '11 at 18:50

2 I like the following slight rephrasing. Suppose the number of primes is finite, say C. Every $n \in \{1, \ldots, N\}$ can be written uniquely in the form $k^2\ell$ where ℓ is a product of distinct primes. The number of choices for k is at most $\sqrt{N}$, and the number of choices for ℓ is at most 2^C. Therefore the number of integers in $\{1, \ldots, N\}$ is at most $2^C\sqrt{N}$, which clearly cannot remain true as N increases. – idmercer Jul 8 '11 at 0:44

I prefer his phrasing, no offense. – Patrick Da Silva Jul 9 '11 at 22:16

Proof 3 is due to Fürstenberg (see also the Wikipedia page) and is honestly not that different from Euclid's proof. See this MO question and the corresponding links for an extended discussion.

I give a counting proof here that I think should be better-known. Briefly, let $\pi(n)$ denote the number of primes less than or equal to n. The prime factorization of any positive integer less than or equal to n has the form $\prod p_k^{e_k}$ where

$$\sum_{k=1}^{\pi(n)} e_k \log p_k \leq \log n$$

so it follows that $e_k \leq \log_2 n$ for all k, hence that $n \leq (\log_2 n + 1)^{\pi(n)}$. This gives the following extremely weak version of the PNT:

$$\pi(n) \geq \frac{\log n}{\log(\log_2 n + 1)}.$$

One can use the same idea to prove that any strictly increasing sequence of positive integers which is polynomially bounded has the property that infinitely many primes divide one of its terms, which is stronger than what can be achieved using Euclid's proof (which only gets you this result for polynomials).

Edit: According to Pete Clark's notes, the above proof was in some form given by (but does not seem to be originally due to) Chaitin. In his formulation it can be summarized using the following slogan: if there were finitely many primes, then the prime factorization of a number would be too efficient a way of representing it. This is quite a nice slogan in that it immediately suggests the generalization to polynomially bounded sequences.

edited Jul 7 '11 at 16:27 — community wiki — 5 revs, 2 users 96% — Qiaochu Yuan

I added two links to Fürstenberg's proof. I hope you don't mind. – t.b. Jul 7 '11 at 4:52

Whew. Nice. Seriously, reading all those proofs, I remember other proofs. XD Giving you the green check Qiao :) thanks a lot – Patrick Da Silva Jul 7 '11 at 5:03

3 @Patrick: don't take this the wrong way, but I don't really understand the point of accepting an answer to a big-list question... – Qiaochu Yuan Jul 7 '11 at 5:11

It's just a way of giving extra rep. I'm being thankful. You gave me like four proofs. – Patrick Da Silva Jul 7 '11 at 5:23

7 @Patrick: I think you will get more answers if you don't accept an answer. More answers accumulating means more people get to learn about interesting proofs, which is much more important than reputation. I'm not sure accepting CW answers gives reputation, and even if it did I don't really need it... – Qiaochu Yuan Jul 7 '11 at 5:24

|

Source : *Proofs from the Book*, by Martin Aigner and Günter M. Ziegler.

Here is one more proof. I don't really know who discovered it.

> Let $\pi(x) = \#\{\text{No of primes } \leq x\}$. Suppose p is the largest element. We consider the Mersenne number $2^p - 1$, and show that for any prime factor q of $2^p - 1$ is bigger than p. So let p be a prime dividing $2^p - 1$. So we have $2^p \equiv 1 \pmod{q}$. Since p is prime, his means

> that, the element 2 has order p in the multiplicative group $\mathbb{Z}_q \setminus \{0\}$ of the field $\mathbb{Z}_q$. This group has $q-1$ elements, so by Lagrange's theorem, we know that the order of every element divides the order of the group. Hence $p \mid (q-1)$, which shows that $p < q$.

Added.

> - Please see: **Three Forgotten Proofs,** Page 10, Book: *The Little Book of Bigger Primes* by Paulo Ribenboim.

edited Jul 7 '11 at 10:30 — community wiki, 5 revs, 3 users 71%, user9413

8 Ugh. Chandru, you have been warned time and time again about citing your sources. This is, nearly word for word, the second proof in *Proofs from the Book*. – Qiaochu Yuan Jul 7 '11 at 5:27

9 @chandru: "How am I to remember the fact where I had taken this from." You don't seem to understand that it is your responsibility to remember this, or at least not to reproduce things when you know you have a habit of verbatim copying. This same attitude applied to your written work would get you kicked out of many if not most universities. – Pete L. Clark Jul 7 '11 at 6:40

3 Here is the source. As Qiaochu said, it is almost verbatim copying. – Zev Chonoles Jul 7 '11 at 6:55

4 Saying you don't know to whom the proof is due allows for the possibility that you wrote up the argument yourself. (For instance, a mathematically equivalent version of this same proof appears in the document linked to in my answer, but the argument has been rewritten in my own words.) Even to say "I took this almost verbatim from somewhere, but I can't remember where" is not a good practice, because you took the time to copy something without taking the care to record what you were copying. If others can catch you out, then with the same amount of effort you can retrieve your sources. – Pete L. Clark Jul 7 '11 at 7:39

3 @Chandru: the post is much better now. Thank you for taking our concerns seriously. – Pete L. Clark Jul 9 '11 at 15:20

|

One proof approach is to construct an infinite set of numbers, any two of which are relatively prime. The proof using Fermat numbers/Euclid's proof can be considered to follow that approach (so I am not sure if I should even be adding this answer!).

We construct a set explicitly as follows.

Start with 3. Now if we already have $\{x_1, x_2, \ldots, x_n\}$ so far, whose prime divisors are $\{p_1, p_2, \ldots, p_r\}$, take $x_{n+1} = 2^{(p_1-1)(p_2-1)\ldots(p_r-1)} + 1$

By Fermat's little theorem, $x_{n+1} = 1 \mod p_i$ and thus is relative prime to each x_i.

Incidentally the Fermat numbers are relative co-prime can also be proved as follows:

If $x = 2^{2^m}$ and $2^{2^m} + 1 = 0 \mod p$, (i.e. $x = -1 \mod p$) then since 2^{2^n} is an even power of x, we have that $2^{2^n} + 1 = 2 \mod p$.

edited Jul 7 '11 at 6:00 — community wiki, 2 revs, Aryabhata

This is the idea behind the two proofs in my question ; the one with the sequence $2^{2^n}+1$ and the other one with the Chinese Remainder Theorem. But the approach with your x_{n+1} I didn't know, thanks. – Patrick Da Silva Jul 7 '11 at 20:14

Here's a proof in the language of ring theory. By the division algorithm, $\mathbb{Z}$ is a principal ideal domain. Thus its maximal ideals are precisely those nonzero of the form (p) where p is prime.

Assume for contradiction that there are finitely many primes $p_1, \ldots, p_n$. Then the product $j = p_1 \cdots p_n$ lies in every maximal ideal of $\mathbb{Z}$, hence in its Jacobson radical. It follows that $1 + j$ is a unit in $\mathbb{Z}$. But this is absurd, not least because $1 + j > 1$.

(While poking around to see if the proof had already appeared on this site, I also stumbled on a very nice result by Bill Dubuque that an infinite ring with "fewer units than elements" has infinitely many maximal ideals. Apparently, this strengthens an argument by Kaplansky.)

answered Jan 23 '14 at 3:36 — community wiki, Manny Reyes

But I think that if you reformulate the actual arguments by translating all the "language" you use, this is Euclid's proof. Doesn't mean I don't like the translation though! – Patrick Da Silva Jan 25 '14 at 0:10

Another well-known proof which is somewhat related to two of the proofs by Qiaochu above is to note that for every prime $p \leq n$, the power of p dividing $n!$ is at most $p^{\frac{n-1}{p-1}}$. Since certainly $n^{\frac{1}{n-1}} < 2$, we obtain that $2^{n\pi(n)} > n!$, where $\pi(n)$ is the number of primes less than or equal to

$p^{p-1} \geq 2$, we obtain that $2^{\pi(n)} \geq n!$, where $\pi(n)$ is the number of primes less than or equal to n. Using Stirling's formula shows that $\pi(n) \to \infty$ as $n \to \infty$. A more careful version of this argument goes back to Chebyshev.

In an AMM paper (around 1954) called "A Method for finding primes", John Thompson came up with a simple, but very nice, variant of Euclid's argument: if we list a set of distinct primes, $\{p_1, p_2, \ldots, p_n\}$, not necessarily in increasing order, then for any $k \leq n$, the integer $p_1 \ldots p_k - p_{k+1} \ldots p_n$ is not divisible by any of the given p_i. This may be ± 1, of course, but in that case you can interchange various p_i's. The point is that you get lots more primes not in your original list this way, and they are divisors of numbers not necessarily so much larger than the primes you start with.

edited Jul 8 '11 at 7:44 — community wiki, 2 revs, Geoff Robinson

3 You don't need the full strength of Stirling's formula; using the fact that $e^x \geq \frac{x^n}{n!}$ for $x \geq 0$ we get $e^n \geq \frac{n^n}{n!}$ or $n! \geq \left(\frac{n}{e}\right)^n$. I learned this argument from Terence Tao's very nice post here: terrytao.wordpress.com/2010/01/02/… – Qiaochu Yuan Jul 7 '11 at 13:16

Yes. Nice simplification, thanks. – Geoff Robinson Jul 7 '11 at 13:50

There's a collection at http://primes.utm.edu/notes/proofs/infinite/

answered Jul 7 '11 at 4:44 — community wiki, Gerry Myerson

Actually four of the five proofs there are in my question, but I like the fifth one! – Patrick Da Silva Jul 7 '11 at 5:00

The following proof can be extracted from Erdős' proof of Bertrand's postulate (although perhaps this argument should be credited to Chebyshev). We need the following two lemmas from that page.

Lemma 1: $\binom{2n}{n} > \frac{4^n}{2n+1}$.

Lemma 2: The greatest power $R(p,n)$ of a prime p dividing $\binom{2n}{n}$ satisfies $p^{R(p,n)} \leq 2n$.

From these two lemmas it follows that

$$\frac{4^n}{2n+1} < \binom{2n}{n} \leq (2n)^{\pi(2n)}$$

which is a contradiction for large n if $\pi(2n)$ is bounded. This gets us within a constant of the PNT:

$$\pi(2n) \geq \frac{n \log 4 - \log(2n+1)}{\log 2n}.$$

edited Jul 7 '11 at 5:19 — community wiki, 2 revs, Qiaochu Yuan

This is taken from Section 1.4 of Andrew Granville's notes on Prime numbers:

> We finish this section by proving that for any $f(t) \in \mathbb{Z}[t]$ of degree ≥ 1 there are infinitely many distinct primes p for which p divides $f(n)$ for some integer n. We may assume that $f(n) \neq 0$ for all $n \in \mathbb{Z}$ else we are done. Now suppose that $p_1, \ldots, p_k$ are the only primes which divide values of f and let $m = p_1 \cdots p_k$. Then $f(nmf(0)) \equiv f(0) \pmod{mf(0)}$ for every integer n, by exercise 1.2a.a, so that $f(nmf(0))/f(0) \equiv 1 \pmod{m}$. Therefore $f(nmf(0))$ has prime divisors other than those dividing m for all n but the finitely many n which are roots of $(f(tmf(0)) - f(0))(f(tmf(0)) + f(0))$, a contradiction.

Exercise 1.2a.a is: Prove that if $f(t) \in \mathbb{Z}[t]$ and $r, s \in \mathbb{Z}$ then $r - s$ divides $f(r) - f(s)$.

Other parts of his course notes might be interesting in connection with this question, too.

answered Nov 27 '11 at 12:11 — community wiki, Martin Sleziak

1 Funny you should say that, Andrew's my advisor. XD Thanks! – Patrick Da Silva Nov 27 '11 at 18:19

Prove infinite number of primes using Wilson's Theorem and Euclid's argument:

Let P be the maximum prime number. From Wilson's Theorem, P is prime if and only if $P \mid (P-1)! + 1$. Thus, $(P-1)! + 1 = kP$, for some natural number k.

Let $n > P$ since there are infinite natural numbers,

$(n-1)! + 1 = rs$, for some natural numbers r & s.

If $r = n$ or $s = n$, then n is prime (Wilson's Theorem) & $n > P$ (proven).

If both r and s are not equal to n, let r represents one of the prime factor of $(n-1)! + 1$.

r cannot be 2 to $(n-1)$, otherwise $r \mid (n-1)!$ and $r \mid [(n-1)! + 1]$ at the same time then $r \mid 1 \rightarrow\ r = 1$, which is impossible.

So this prime factor r is not from 2 to n; it is another prime $> n > P$.

Leow (2013)

edited Dec 18 '13 at 6:39

community wiki
2 revs, 2 users 82%
Prime Leow

Let P be a polynomial with integer coefficients a_d and degree n. Then

$$I(P) = \int_0^1 P(x)dx = \sum_{k=0}^{n} \frac{a_k}{k+1}$$

If $I(P) \neq 0$ then multiplying by $L = \operatorname{lcm}[1, 2, \ldots, n+1]$ we get

$$L \cdot |I(P)| \geq 1$$

because $L \cdot I(P)$ is an integer. Now note that

$$L = \exp(\psi(n+1))$$

where $\psi(n) = \sum_{p^k \leq n} \log p$. Therefore

$$\exp(\psi(n+1)) \geq \frac{1}{|I(P)|}$$

Choose $P(x) = x^m(1-x)^m$. Then on $0 < x < 1$ we have $|P(x)| \leq 2^{-2m}$. Therefore $|I(P)| \leq 2^{-2m}$. Therefore

$$\psi(2m+1) \geq 2m \log 2$$

This proves the infinitude of the primes. In fact it proves more, it proves the Chebychev bound

$$\pi(x) \gg x/\log x$$

This proof cannot be refined to a proof of the prime number theorem. The optimal choice of the polynomial gives only a constant of $0.86\ldots$ in place of $\log 2$.

REFERENCES: Chapter 10 of Montgomery's book "Ten lectures on the interface between harmonic analysis and analytic number theory".

EDIT: Here are the details of the $\gg$ bound. Note that $\psi(2m+1) \geq 2m \log 2$ implies $\psi(x) \gg x$ for all x. The prime squares and higher contribute $O(\sqrt{x} \log x)$ to $\psi(x)$ and the primes p contributes at most $\pi(x) \log x$ since each $\log p \leq \log x$. Therefore

$$\pi(x) \log x + \sqrt{x} \log x \gg \psi(x) \gg x$$

Hence

$$\pi(x) \gg x/\log x$$

edited Jun 30 '13 at 2:20

community wiki
3 revs
blabler

I don't see how this proves the lessthan-lessthan bound. Can you explain in more detail? I'm interested. – Patrick Da Silva Jun 30 '13 at 0:46

Yes of course! It's a rather standard derivation but I'll include it in the edits. – blabler Jun 30 '13 at 1:54

At least to me this proof has a touch of transcendental number theory: First, the use of the fact that a non-zero integer has to be in absolute value ≥ 1. Secondly, the optimization problem involving a choice of a polynomial with integer coefficients. – blabler Jun 30 '13 at 2:12

Am I supposed to read the reference to understand the proof better? Because right now I don't get it. Maybe it feels trivial to you but it's not to me. – Patrick Da Silva Jun 30 '13 at 3:00

Thanks for fixing the details. Took me a while to understand that $\psi(n)$ function actually! I didn't read it well enough the first time. – Patrick Da Silva Jun 30 '13 at 3:08

There is a very clever one-line proof which I can't understand why it's not here. The Proof:

$$0 < \prod_p \sin\left(\frac{\pi}{p}\right) = \prod_p \sin\left(\frac{\pi(1 + 2\prod_{p'} p')}{p}\right) = 0.$$

This proof has created by Sam Northshield in 2015 and published in American Mathematical Monthly.

answered Feb 13 at 19:51 community wiki Mathelogician

The inequality is because you are taking a product of positive numbers. The first equality is because the product of all p' is divisible by p, so the argument is congruent to π/p modulo 2π. The last equality is because the integer $1 + 2\prod$ is divisible by some prime, hence the factor corresponding to it vanishes. I remember seeing this proof, it's a nice one! – Patrick Da Silva Feb 13 at 19:55

I don't see how you can prove that (1+2∏p')/p is an integer. The p in the denominator isn't "any" p. It's each and every p. – Aheho Mar 15 at 4:21

Let p be the last prime. Then according to Bertrand's postulate the interval $(p, 2p)$ contains a prime number. We get a contradiction.

edited Feb 28 '16 at 12:57 community wiki 2 revs, 2 users 67% Leox

Proofs from the book has already been mentioned so it seems silly to spell out yet another proof from that source, but on the other hand I feel that this proof deserves special mentioning since it has two rather striking properties:

1) Like you mention in your post the point of many proofs is the construction of a sequence of numbers in which each member a_n is coprime to each of the (finitely many) previous ones. A special feature of this proof is that it shows this fact (for a special sequence $a_1, a_2, a_3, \ldots$) by showing that a_n is comprime to all the (infinitely) a_m *succeeding it*. The fact that both properties of a_n are equivalent is of course completely elementary but still I found it initially hard to get my head around. And intuitively it is of course weird that it is easier to prove a number coprime to an infinite set of numbers (its successors) than to a finite set of numbers (it predecessors).

2) The proof relies on a mathematical fact that is very dear to me (and probably many mathematicians) as it was the first truly beautiful formula I discovered myself:

$$2 + 2 = 2 * 2$$

Of course, being older and wiser, this looks like a 'strong law of small numbers'-type phenomenon rather than a deep equation, so i was all the more happy to see it used as the fundament of a proof of one of the most celebrated facts of mathematics.

So here goes the proof:

Start with an odd number a_1 and construct an infinite sequence of odd numbers by

$$a_{n+1} = a_n^2 - 2$$

To see that a_n has no common divisors with its successors let q be a prime divisor of a_n. It suffices to show that no a_m is never congruent $0 \mod q$ for $m > n$. Well, $a_{n-1} \equiv -2 \mod q$ and, courtesy of the above mentioned beautiful formula, $a_m \equiv 2 \mod q$ for every $m \geq 2$. q being odd this proves the claim.

answered Jan 18 '14 at 21:49 community wiki Vincent

To be honest, I'm not really... impressed. But I'm happy you're amazed. – Patrick Da Silva Jan 19 '14 at 0:41

Well of course after Euclid every proof consisting of constructing an infinite sequence of mutually coprime integers is a bit derivative. What would be truly impressive is to have a proof that does not rely on the fact that every sufficiently large number is divisible by at least one prime, but I don't think such a proof can exist. – Vincent Jan 19 '14 at 12:59

Um... Every number not in $\{-1, 0, 1\}$ is divisible by at least one prime. If by sufficiently large you mean ≥ 2 that's a fancy way to say it. Otherwise, the topological proof ultimately does that ; it only secretly uses the fundamental theorem of arithmetic, but not in a very deep way. It is definitely my favorite. – Patrick Da Silva Jan 19 '14 at 14:14

Ha, I meant ≥ 2 but wrote it in a fancy way pretty much because of the topological proof: until I read your comment I believed the topological proof ultimately used that the set of numbers not divisible by any prime is finite (rather than being just $\{-1, 1\}$ which of course also is true). Now however I realize that (even better) it only needs the set of numbers not divisible by any prime to be not-open in this special topology, which is a much weaker statement. I wonder if there is a non-euclidean ring in which this

topology, which is a much weaker statement. I wonder if there is a non-euclidean ring in which this distinction can be made explicit. Anyway: thank you for this insight! – Vincent Jan 19 '14 at 14:57

To clarify: what I meant with my last question is 'is there a non-noetharian ring in which the set of elements not divisible by any irreducible element is infinite but not open in the topology generated by cosets of ideals?' If I understand things correctly in such a ring you could use the topological proof to show the existence of infinitely many irreducibles. (Or should I replace irreducibles with primes here to make the proof go through?) Anyway, infinite sequences of coprime elements seem to be quite useless in such a ring... – Vincent Jan 19 '14 at 15:14

|

The following proof use the Euler's totient function and relies on the fact that $\phi(m) > 1$ for all $m \geq 3$.

Assume that there are only a finite number of primes say $p_1, p_2, \ldots, p_k$. Look at the product of these finite primes i.e.

$$m = p_1 p_2 \cdots p_k$$

Now consider any number $n > 1$. Since there are only finite primes, one of the p_j's must divide n. Hence, $\gcd(m, n) > 1$. Hence, $\phi(m) = 1$ contradicting the fact that $\phi(m) > 1$ for all $m \geq 3$.

answered Dec 28 '12 at 21:19 — community wiki — user17762

1 How to prove that $\varphi(m) > 1$ for all $m \geq 3$? For 1 and m-1 are the totative of m?However I need Bezout equation to prove m-1 and m are coprime . – tan9p Dec 26 '14 at 12:39

Maybe you wanna use the sum of reciprocal prime numbers. The argument for the fact that
the series diverges you may find here in one of Apostol's exercise.

edited Dec 29 '12 at 11:13 — community wiki — 2 revs — Chris's wise sister

How about this? Let x be a rational in (0,1). Then x is of the form x = m/M with M>m. If x has a non terminating decimal expansion then x must be of the form x = m/p where p is a prime number. Also, the period of x, say T(x), is less than p. Let A = { x such that x is rational in (0,1) and has non terminating decimal expansion } Let B = { y=T(x) such that x is an element of A } We then have that for every y in B there is at least one prime p and natural m such that y = T(x) = T(m/p) < p Since B is unbounded so is the set of prime numbers

answered Aug 6 '15 at 18:52 — community wiki — DanielHS

The claim

$$x \in \mathbb{Q} \text{ has a non-terminating decimal part } \implies x = \frac{m}{p} \text{ for some prime } p$$

is false. For instance, $x = \frac{1}{90}$ is a counter-example. – G. Sassatelli Aug 6 '15 at 19:22

1 But, for instance, $0,0555555555\ldots = \frac{1}{18}$ and 18 is not prime. I don't think we can write $0,0555555555\ldots$ in the form m/p where p is a prime. – Ramiro Aug 6 '15 at 19:24