A FEW PROOFS OF THE INFINITUDE OF PRIMES (MA2316, THE INTRODUCTORY LECTURE)

VLADIMIR DOTSENKO

Let us outline here a few proofs of the infinitude of primes. Altogether, they give a nice introduction to basic methods of number theory. One of very important arithmetic functions is $\pi(N)$, the number of primes not exceeding N. In other words, we shall show that $\lim\limits_{N\to+\infty}\pi(N)=+\infty$.

Proof 1. (Euclid) Suppose that there are finitely many primes $p_1, \ldots, p_k$. Consider the number $N = p_1p_2\cdots p_k + 1$, and let q be a prime divisor of N. Clearly, $\gcd(N, p_i) = 1$, so q is a prime number different from all p_i. Contradiction. □

Proof 2. Let us show that the Fermat numbers $2^{2^n}+1$ are pairwise coprime. Indeed, because of the formula $(a-b)(a+b)=a^2-b^2$, we have

$$(2-1)(2+1)(2^2+1)(2^4+1)(2^8+1)\cdots(2^{2^n}+1)=2^{2^{n+1}}-1=(2^{2^{n+1}}+1)-2,$$

which shows that any common divisor of $2^{2^{n+1}}+1$ and $2^{2^m}+1$ with $m\leq n$ is a divisor of 2, and hence is equal to 1 since all Fermat numbers are odd. Therefore, different Fermat numbers have different prime divisors, and the number of primes is therefore infinite. □

The two above proofs no not use anything except divisibility. The next one requires a bit of basic group theory.

Proof 3. Let p be a prime number, and let q be a prime divisor of 2^p-1. We shall now show that $q>p$, which will show that there is no largest prime number, and hence prove our result. Since $2^p\equiv 1 \pmod q$, we see that the order of 2 in the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ divides p, hence is equal to p (since p is a prime). By the Lagrange's theorem, p divides the order of the group $(\mathbb{Z}/q\mathbb{Z})^\times$, that is $q-1$. Hence $q>p$. □

The next proof uses basics of analysis.

Proof 4. (Euler) Suppose that there are finitely many primes $p_1, \ldots, p_k$. Let us expand the expression

$$\left(1-\frac{1}{p_1}\right)^{-1}\left(1-\frac{1}{p_2}\right)^{-1}\cdots\left(1-\frac{1}{p_k}\right)^{-1},$$

using the geometric series formula

$$\left(1-\frac{1}{p}\right)^{-1}=1+\frac{1}{p}+\frac{1}{p^2}+\ldots$$

Taking only the terms up to $\frac{1}{p_1^{a_1}}$ in the first series, the terms up to $\frac{1}{p_2^{a_2}}$ in the second series etc., we deduce that

$$\left(1-\frac{1}{p_1}\right)^{-1}\left(1-\frac{1}{p_2}\right)^{-1}\cdots\left(1-\frac{1}{p_k}\right)^{-1}\geq\sum_{n\leq p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}}\frac{1}{n},$$

which is impossible, since the partial sums of the harmonic series $\sum\frac{1}{n}$ increase without bound. □

The next proof is said to be inspired by information theory: the contradiction comes from the fact that if there were only finitely many primes, then large numbers could be represented too economically.

Proof 5. (Chaitin) Suppose that there are finitely many primes $p_1, \ldots, p_k$. Let us estimate the number of integers that do not exceed N that can be formed as products $p_1^{a_1} \cdots p_k^{a_k}$. For a_1, we have at least the restriction $p_1^{a_1} \leq N$, so $a_1 \leq \log_{p_1} N = \frac{\ln N}{\ln p_1}$. Similarly, $a_2 \leq \frac{\ln N}{\ln p_1}$ etc. Therefore, the total number of products we may form is at most

$$\left(1 + \frac{\ln N}{\ln p_1}\right)\left(1 + \frac{\ln N}{\ln p_2}\right) \cdots \left(1 + \frac{\ln N}{\ln p_k}\right),$$

hence

$$N \leq \left(1 + \frac{\ln N}{\ln p_1}\right)\left(1 + \frac{\ln N}{\ln p_2}\right) \cdots \left(1 + \frac{\ln N}{\ln p_k}\right).$$

But the latter inequality would mean that a polynomial in $\ln N$ grows faster than N, which is impossible since for each fixed k we have

$$\lim_{N \to +\infty} \frac{\ln^k N}{N} = 0.$$

□

Proof 6. (Erdös) Let us note that each positive integer n can be uniquely decomposed as $N = rs^2$, where r is square-free, that is not divisible by a perfect square greater than 1. From that, it follows that

$$N \leq 2^{\pi(N)} \cdot \sqrt{N}.$$

Indeed, the left hand side is the number of positive integers not exceeding N, and the right hand side estimates that number. A square free number is a product of distinct primes, and to get an estimate from above, we may just take or not take any prime not exceeding N (which accounts for the $2^{\pi(N)}$ factor), and also there are at most $\sqrt{N}$ perfect squares not exceeding N. Simplifying, we conclude that

$$2^{\pi(N)} \geq \sqrt{N},$$

hence $\lim_{N \to +\infty} \pi(N) = +\infty$. □

Let us remark that from this proof it is very easy to deduce that the sum of reciprocals of primes is infinite. For otherwise we would have

$$\sum_{p > p_k} \frac{1}{p} < \frac{1}{2}$$

for some k. Note that the number of integers not exceeding N that are divisible by p is at most $\frac{N}{p}$, therefore, the number of integers not exceeding N that have a prime divisor $p > p_k$ is at most

$$\sum_{p > p_k} \frac{N}{p} < \frac{N}{2}.$$

This implies that for any N, at least half of integers not exceeding N only have prime divisors not exceeding p_k, which gives

$$\frac{N}{2} \leq 2^k \cdot \sqrt{N},$$

a contradiction.

The next proof is a slick combination of the fourth and the sixth one.

Proof 7. Let us note that since each positive integer n can be uniquely decomposed as $N = rs^2$, where r is square-free, the sum of reciprocals of square-free numbers

$$\sum_{r \text{ square-free}} \frac{1}{r}$$

is infinite, otherwise the harmonic series

$$\sum \frac{1}{n} = \sum_{r \text{ square-free}} \frac{1}{r} \cdot \sum \frac{1}{s^2}$$

would have been convergent. But if there are finitely many primes $p_1, \ldots, p_k$, then we have

$$\sum_{r \text{ square-free}} \frac{1}{r} = \left(1 + \frac{1}{p_1}\right)\left(1 + \frac{1}{p_2}\right) \cdots \left(1 + \frac{1}{p_k}\right),$$

a contradiction. □

The last proof is probably the most bizarre one since it uses notions of basic topology.

Proof 8. (Fürstenberg) Let us call a subset $U \subset \mathbb{Z}$ open, if it is empty, or a union of arithmetic sequences. In other words, a set of integers is open if together with every number x it contains some arithmetic sequence $x + an$, $n \in \mathbb{Z}$. The set of all integers together with this collection of open sets forms a *topological space*, that is open sets satisfy the three key properties that open sets always satisfy:

- The sets $\varnothing$ and $\mathbb{Z}$ are open, the former by definition, the latter because it is an arithmetic sequence.
- A union of several open sets is open: a union of unions of arithmetic sequences is a union of arithmetic sequences.
- A finite intersection of several open sets is open. Indeed, if $x \in U_1 \cap U_2 \cap \cdots \cap U_k$, then x belongs to each U_l, and hence U_l contains some arithmetic sequence $x + a_l n$, $n \in \mathbb{Z}$. But then $U_1 \cap U_2 \cap \cdots \cap U_k$ contains the arithmetic sequence $x + \operatorname{lcm}(a_1, \ldots, a_k)n$, $n \in \mathbb{Z}$.

Note that the set of integers that are *not* divisible by the given number m is open: is is the union of arithmetic sequences $k + mn$, $n \in \mathbb{Z}$, for all $k = 1, \ldots, m-1$. Therefore, if there were finitely many different primes $p_1, \ldots, p_k$, then the set of integers not divisible by any of them would have been open, as a finite intersection of open sets. But this set is manifestly $\{-1, 1\}$, so it definitely is not open (nonempty finite sets are not open for this topology. □

There are some reasons to think that Fürstenberg's proof is Euclid's proof in disguise. Indeed, one can argue the set of integers that are not divisible by p_l contains 1, so unwrapping the lcm construction above, we conclude that the set of integers not divisible by any of p_l contains $1 + p_1 p_2 \cdots p_k$, which must have prime divisors, and that leads to a contradiction. However, at this stage we are making a choice that brings the proofs together. However, on the nose, Fürstenberg's proof obtains a contradiction in a much more non-constructive way than the Euclid's one.

Remark. *Let us show that Fürstenberg's topology actually comes from a certain metric on $\mathbb{Z}$. For $x, y \in \mathbb{Z}$, let us define*

$$d(x, y) = \begin{cases} 0, x = y, \\ \frac{1}{\max\{k! \colon k! | (x-y)\}} \end{cases}$$

(we leave it as an exercise to check that this $d(x, y)$ satisfies all axioms of a metric). Note that the open ball of radius $\frac{1}{(m-1)!}$ centered at the point x of this metric space is precisely the the arithmetic sequence $x + m!\mathbb{Z}$. Thus, each open ball in this metric space contains an arithmetic sequence, and each arithmetic sequence contains an open ball, so an open set in this metric space is precisely an open set as defined in Fürstenberg's proof.