My Favourite Proofs of the Infinitude of Primes

Chris Almost

November 23, 2005

The following proofs depend on the fact that the positive integers grow without bound, and on the following simple lemma.

Lemma 1. *If $n \in \mathbb{Z}$ and $|n| \neq 1$ then there is prime number that divides n.*

Proof. Every prime divides 0, so suppose n is minimal such that $|n| \neq 1$ and there is no prime dividing n. Then n is not prime (since it divides itself) so it is composite. Suppose $n = ab$, where $|a| \neq 1$ and $|b| \neq 1$, so $|a| < |n|$ and $|b| < |n|$. By minimality of n, there is a prime that divides a. But this prime will then divide n, a contradiction showing that there is no such n. □

Theorem (Euclid)**.** *There are infinitely many prime numbers.*

A Proof from Topology

Definition 1. Let X be a set and $\mathcal{T}$ be a collection of subsets of X. $\mathcal{T}$ is a *topology* on X if

O1. $\emptyset, X \in \mathcal{T}$

O2. If $\{U_\alpha\}_{\alpha \in A} \subseteq \mathcal{T}$ then $\bigcup_{\alpha \in A} U_\alpha \in \mathcal{T}$

O3. If $U, V \in \mathcal{T}$ then $U \cap V \in \mathcal{T}$.

The elements of $\mathcal{T}$ are the *open sets* of the *topological space* $(X, \mathcal{T})$. The complements of the open sets are the *closed sets*

Proof (Fürstenburg, 1955). Consider the topology on $\mathbb{Z}$ defined by taking unions of sets of the from $U_{a,b} = \{n \mid n \equiv a \pmod{b}\}$. If O_1 and O_2 are such sets and $x \in O_1 \cap O_2$ then $U_{x,b_1} \subseteq O_1$ and $U_{x,b_2} \subseteq O_2$ for some b_1 and b_2. But then $U_{x,\operatorname{lcm}\{b_1,b_2\}} \subseteq O_1 \cap O_2$, which shows that $O_1 \cap O_2$ is open, so this is indeed a topology.

Each basic open set $U_{a,b}$ is also closed since

$$\mathbb{Z} \setminus U_{a,b} = \bigcup_{\substack{i=0 \\ i \neq a}}^{b-1} U_{i,b}$$

i.e. the compliment of $U_{a,b}$ can be written as a a union of open sets. Suppose there are finitely many primes. Let

$$A := \bigcup_{p \text{ prime}} U_{0,p}$$

By assumption, A is closed since it is a finite union of closed sets. By Lemma 1, $\mathbb{Z} \setminus A = \{1, -1\}$. But every non-empty open set is infinite, so this is a contradiction and A cannot be closed. Therefore there are infinitely many primes. □

A Proof from Group Theory

Definition 2. A *group* is a set G together with a binary operaration $\cdot : G \times G \to G$ such that

G1. $\cdot$ is associative.

G2. There is an element $e \in G$ such that for every $a \in G$, $a \cdot e = a = e \cdot a$; the *indentity element.*

G3. For every element $a \in G$ there is $b \in G$ such that $a \cdot b = e = b \cdot a$; the *inverse of* a.

A *subgroup* H of G is a subset of G that is a group with respect to the restricted binary operation.

Theorem (Lagrange)**.** *If G is a finite group and H is a subgroup of G then the order of H divides the order of G.*

Proof of Euclid's Theorem. Suppose that p is the largest prime. Let q be a prime factor of the number $2^p - 1$ (this is a *Mersenne number*). Then $2^p \equiv 1 \pmod{q}$, so the order of the element 2 in the group $(\mathbb{Z}/q\mathbb{Z})^*$ divides p. But p is prime, so the order of 2 is p, and p divides $q - 1 = |(\mathbb{Z}/q\mathbb{Z})^*|$ by Lagrange's Theorem. Hence $p < q$, a contradiction since p was supposed to be the largest prime. □

A Proof Using Fermat Numbers

Recall that $x^2 - 1 = (x - 1)(x + 1)$.

Proof (Goldbach, 1970). A *Fermat number* is a number of the from $F_n = 2^{2^n} + 1$. Notice that

$$F_n - 2 = 2^{2^n} - 1 = (2-1)(2+1)(2^2+1)\cdots(2^{2^{n-2}}+1)(2^{2^{n-1}}+1) = \prod_{i=0}^{n-1} F_i$$

So if p is prime that divides F_m then p cannot divide F_n for any $n > m$ since then p would divide 2, a contradiction since all Fermat numbers are odd. Since there are infinitely many Fermat numbers there must be infinitely many primes. □