INFINITUDE OF PRIMES

STEVEN V SAM

We aim to present as many interesting proofs of the following theorem as possible. This list is very short, so please inform me of any others you might know. I’m mainly interested in proofs from different areas of math, and am aware that there are many variations of number-theoretic arguments given below.

Theorem 1 (Euclid). There are infinitely many primes.

1. Number Theory

Proof. (Euclid) Let \( p_1, \ldots, p_n \) be some distinct primes. We’ll construct another prime \( p_{n+1} \). This process will be independent of \( n \), so it will follow that there must be infinitely many primes. The number \( N = p_1 \cdots p_n + 1 \) is not divisible by any \( p_i \). So either \( N \) is prime in which case we set \( p_{n+1} = N \), or \( N \) is divisible by some prime other than the \( p_i \), which we may call \( p_{n+1} \).

Proof. (Goldbach) Consider the Fermat numbers \( F_n = 2^{2^n} + 1 \). We first show that

\[
F_n - 2 = F_0 F_1 \cdots F_{n-1}.
\]

For \( n = 1 \), this is clear. By induction,

\[
F_n - 2 = F_0 F_1 \cdots F_{n-1},
\]

so

\[
F_n^2 - 2F_n = F_0 F_1 \cdots F_{n-1} F_n.
\]

But

\[
F_n^2 - 2F_n = 2^{2^n+1} + 2^{2^n+1} + 1 - 2^{2^n+1} - 2 = 2^{2^n+1} - 1 = F_{n+1} - 2,
\]

which proves the inductive step. Now these numbers must be relatively prime. For if there exists \( n \) and \( m \) with \( m < n \) such that \( F_m \) and \( F_n \) have a common factor \( d \), then \( d \) divides \( F_0 F_1 \cdots F_{n-1} \) and hence divides \( F_n - F_0 F_1 \cdots F_{n-1} = 2 \). Since each \( F_n \) is odd, \( d = 1 \). Now since we have constructed an infinite sequence of relatively prime numbers, there must be an infinite number of primes.

2. Analysis

Proof. (Euler) Suppose there are finitely many primes \( p_1, \ldots, p_n \). Consider the series

\[
\frac{1}{1 - \frac{1}{p_i}} = \sum_{k \geq 0} \frac{1}{p_i^k}.
\]

By unique factorization,

\[
\prod_{i=1}^{n} \frac{1}{1 - \frac{1}{p_i}} = \sum_{k \geq 1} \frac{1}{k}.
\]

But the left hand side is a finite number, while the right hand side is the divergent harmonic series.

\[Date: \] August 11, 2010.
Proof. (Perott) Suppose there are finitely many primes \( p_1, \ldots, p_n \). Pick \( N > p_1 \cdots p_n \). The number of integers \( m \leq N \) not divisible by a square is \( 2^n \) (the possible number of ways to multiply distinct primes). The number of integers \( m \leq N \) divisible by some square \( p_i^2 \) is at most \( \sum_{i=1}^n N/p_i^2 \). So we get the inequality

\[
N \leq 2^n + \sum_{i=1}^n \frac{N}{p_i^2} < 2^n + N \sum_{k \geq 2} \frac{1}{k^2} = 2^n + N \left( \sum_{k \geq 1} \frac{1}{k^2} - 1 \right) = 2^n + N(1 - \delta)
\]

where \( \delta > 0 \) because

\[
\sum_{k \geq 1} \frac{1}{k^2} < 1 + \sum_{k \geq 1} \frac{1}{k(k+1)} = 1 + \sum_{k \geq 0} \left( \frac{1}{k} - \frac{1}{k+1} \right) = 2.
\]

For sufficiently large \( N \), \( N\delta > 2^n \), which contradicts the above inequality.  

3. Topology

Proof. (Furstenberg [Fur]) Consider \( \mathbb{Z} \) with the topology generated by open sets of the form \( \{ar + b \mid r \in \mathbb{Z} \} \) where \( a, b \in \mathbb{Z} \). Note that any nonempty open set must be infinite. Now note that these basic opens are also closed because they are the complement of

\[
\bigcup_{k=1}^{a-1} \{ar + k \mid r \in \mathbb{Z} \}.
\]

In particular, if there are finitely many primes \( p_1, \ldots, p_n \), then

\[
\mathbb{Z} \setminus \{1, -1\} = \bigcup_{i=1}^n \{p_i r \mid r \in \mathbb{Z} \}
\]

is a closed set, which contradicts that nonempty open sets are infinite.  

Acknowledgements. Thanks go to Pete Clark for pointing out that a previous argument that I made using commutative algebra was circular. 

References