Sketch of Lecture 1

Tue, 8/16/2016

1 Basic proof techniques

1.1 Proofs by contradiction

- $\mathbb{N}=\{1,2,3,\ldots\}$ are the **natural numbers**, and $\mathbb{Z}=\{0,\pm1,\pm2,\ldots\}$ the **integers**.
- $\mathbb{Q}=\left\{\frac{p}{q}:\ p\in\mathbb{Z},q\in\mathbb{N}\right\}$ are the **rationals**, and $\mathbb{R}$ are the **reals** (limits of sequences of rationals).

Example 1. $\sqrt{5}$ is not rational.

Proof. Assume (for contradiction) that we can write $\sqrt{5}=\frac{n}{m}$ with $n,m\in\mathbb{N}$. By canceling common factors, we can ensure that this fraction is reduced.

Then $5m^2=n^2$, from which we conclude that n is divisible by 5. Write $n=5k$ for some $k\in\mathbb{N}$. Then $5m^2=(5k)^2$ implies that $m^2=5k^2$. Hence, m is also divisible by 5. This contradicts the fact that the fraction n/m is reduced. Hence, our initial assumption must have been wrong. □

Variations. Does the same proof apply to, say, $\sqrt{7}$? Which step of the proof fails for $\sqrt{4}$?

Definition 2. An integer $p>1$ is a **prime** if its only positive divisors are 1 and p.

Example 3. (Euclid) There are infinitely many primes.

Proof. Assume (for contradiction) there is only finitely many primes: $p_1,p_2,\ldots,p_n$.
Consider the number $N=p_1\cdot p_2\cdot\ldots\cdot p_n+1$.
Each prime p_i divides $N-1$ and so p_i does not divide N.
Thus any prime dividing N is not on our list. Contradiction. □

Historical note. This is not necessarily a proof by contradiction, and Euclid (300BC) himself didn't state it as such. Instead, one can think of it as a constructive machinery of producing more primes, starting from any finite collection of primes.

A variation. Can we replace $N=p_1\cdot p_2\cdot\ldots\cdot p_n+1$ in the proof with $N=p_1\cdot p_2\cdot\ldots\cdot p_n-1$? Yes! (If $n\geqslant 2$.)

Playing with numbers.

$2+1=3$ is prime. $2\cdot3+1=7$ is prime. $2\cdot3\cdot5+1=31$ is prime. $2\cdot3\cdot5\cdot7+1=211$ is prime. $2\cdot3\cdot5\cdot7\cdot11+1=2311$ is prime. $2\cdot3\cdot5\cdot7\cdot11\cdot13+1=30031=59\cdot509$ is not prime.

Let $P_n=p_1\cdot p_2\cdot\ldots\cdot p_n+1$ where p_i is the ith prime. If P_n is prime, it is called a primorial prime. We have just checked that P_1,P_2,P_3,P_4,P_5 are primes but that P_6 is not a prime.

The next primorial primes are $P_{11},P_{75},P_{171},P_{172}$. It is not known whether there are infinitely P_n which are prime.

More shamefully, it is not known whether there are infinitely many P_n which are not prime.

See, for instance: http://mathworld.wolfram.com/PrimorialPrime.html

1.2 A famous example of a direct proof

Example 4. (Gauss) $1+2+\ldots+n=\frac{n(n+1)}{2}$

Proof. Write $s(n)=1+2+\ldots+n$.
$2s(n)=(1+2+\ldots+n)+(n+(n-1)+\ldots+1)=(1+n)+(2+n-1)+\ldots+(n+1)=n\cdot(n+1)$. Done! □

Anecdote. 9 year old Gauss (1777-1855) and his classmates were tasked to add the integers from 1 to 100 (and not bother their teacher while doing so). Gauss was not writing much on his slate... just the final answer: 5050.

Armin Straub
straub@southalabama.edu