Announcements

- Homework #3 has been posted.
- Homework #2 solutions are posted
- Homework #1 grading will be visible soon

One more Proof of Equivalence

We'll come back to this at the end of the lecture, if time permits.

- Claim: $(\forall n,m \in \mathbb{N})$[n and m have the same "parity" $\leftrightarrow$ n + m is even]

Proof by Contradiction

Sometimes easier than proving something directly:

Claim: **P.**
Proof:
Assume ~P.
…
[Contradiction].
Therefore, P.

Proofs by Contradiction

Lemma 1: $(\forall n \in \mathbb{N})[\ n^2$ even $\leftrightarrow$ n is even$]$

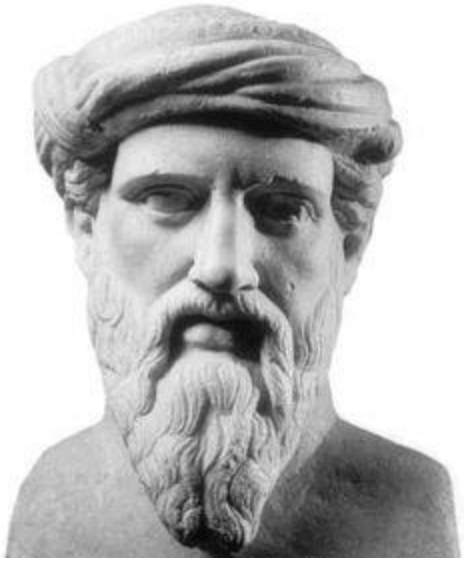
(We already proved this, indirectly. Why?)

- Claim: $(\forall x,y \in \mathbb{Z})[x^2 - 4y \neq 2]$

A Famous Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.

Proven around 500 BC, probably by Hippasus



We'll need these…

Lemma 2: $(\forall x, y \in \mathbb{N}^{>1})$ if $x \mid y$ then $x \nmid (y + 1)$

(Let's prove this…)

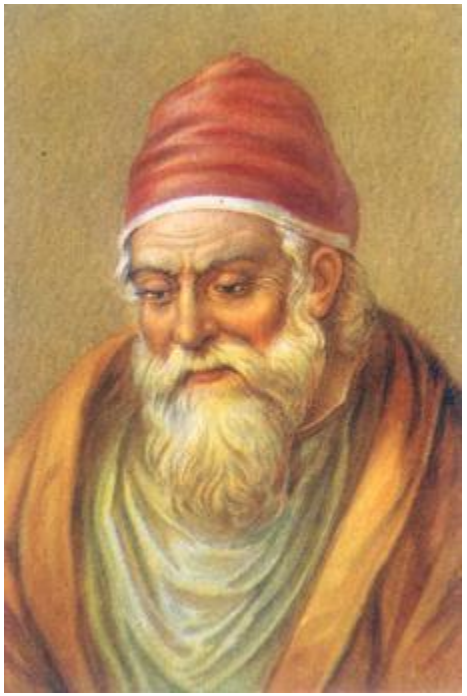
Lemma 3: Every natural number (greater than 1) has a prime factor.

(We'll prove this later…)

Another Famous Proof by Contradiction

Theorem: There are infinitely many primes.

Proven around 300 BC, by Euclid



How Smart is a Computer?

- Can software be written to do certain kinds of proofs?
- Can there be a **TruthMaster®** program that can decide whether or not statements are true in the subject of Number Theory?
- How good can a program be at analyzing source code of other programs?

The Halting Problem

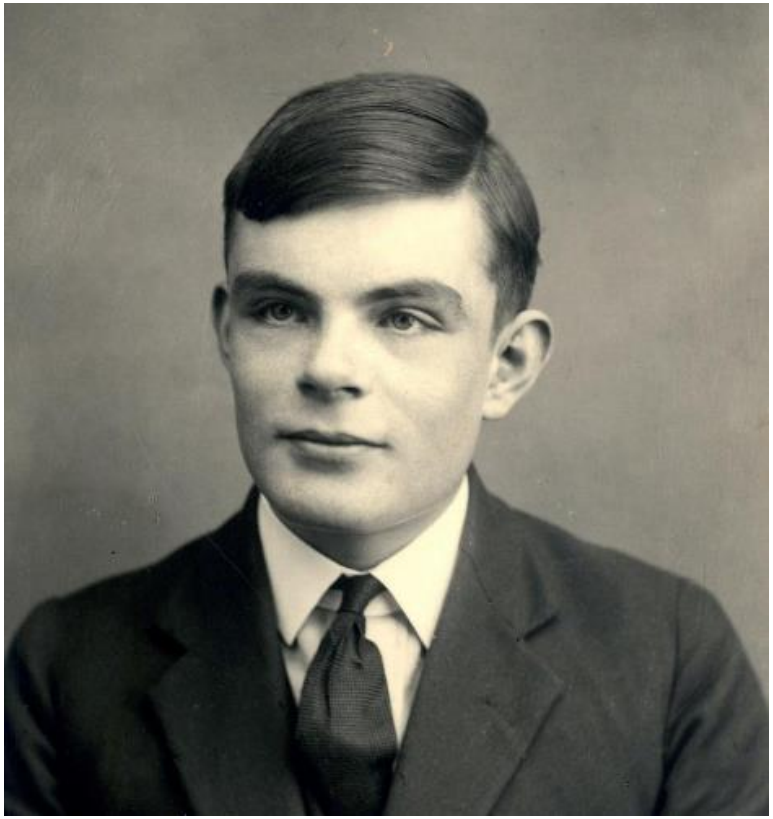
Question: Is it possible to write a computer program called **CodeAnalyzer®** with the following characteristics?

- The CodeAnalyzer program takes two inputs:
  1. Source code of some computer program, P
  2. Data (D) that could be used as input for the program P
- CodeAnalyzer will tell us whether or not the program P would eventually *halt (*when run with input D), by returning either “IT WOULD HALT” or “IT WOULD RUN FOREVER”

Yet Another Famous Proof by Contradiction

Theorem: The "CodeAnalyzer" program cannot exist.

Proven by Alan Turing in 1936. (He was 24 years old.)



Similar Results

Undecidable questions about "What happens when Program P is run on input D":

- Will it halt? (Halting Problem).
- Will it ever reach line 679?
- Will the output include the string "CMSC 250 is fun"?
- Will there be any output?
- Etc.

Math Humor (by Contradiction)

- Claim: All natural numbers are interesting.

Unit 5
Focus on Number Theory

Fundamental Theorem of Arithmetic
(Unique Prime Factorization Theorem)

Theorem: For any $n \in \mathbb{N}$, n can be expressed as the product of primes in a **unique** way.

Examples.

In proofs, we will write:

$$n = p_1^{e1} \times p_2^{e2} \times p_3^{e3} \times \ldots \times p_k^{ek}$$