# Book of Proof: Part III, More on Proof

January 16, 2018

# If-and-Only-If Proof

#### **Outline for If-and-Only-If Proof**

```
Proposition P if and only if Q.

Proof.

"Only if"

[Prove P \Rightarrow Q by whatever means you can.]

"If"

[Prove Q \Rightarrow P by whatever means you can.]
```

**Theorem** Suppose A is an  $n \times n$  matrix. The following statements are equivalent:

- a. A is invertible.
- b. Ax = b has a unique solution for every  $b \in \mathbb{R}^n$ .
- c. Ax = 0 has only the trivial solution.
- d. The reduced row echelong form of A is  $I_n$ .
- e.  $det(A) \neq 0$ .
- f. The matrix A does not have 0 as an eigenvector.

$$a \Rightarrow b \Rightarrow c$$
 $\uparrow \qquad \qquad \downarrow$ 
 $f \Leftarrow e \Leftarrow d$ 

$$\begin{array}{ccccc}
a & \Rightarrow & b & \Leftrightarrow & c \\
\uparrow & & \downarrow & & \\
f & \Leftarrow & e & \Leftrightarrow & d
\end{array}$$

Proposition There exists an even prime number.

Proposition There exists an even prime number.

*Proof.* Two is an even prime number.

**Proposition** There exists an even prime number.

Proof. Two is an even prime number.

**Proposition** There exists an integer that can be expressed as the sum of two perfect cubes in two different ways.

**Proposition** There exists an even prime number.

Proof. Two is an even prime number.

**Proposition** There exists an integer that can be expressed as the sum of two perfect cubes in two different ways. *Proof.* 

$$1^3 + 12^3 = 1729$$
  
 $9^3 + 10^3 = 1729$ 

# Example

**Proposition 7.1** If  $a, b \in \mathbb{N}$  then there exist  $k, \ell \in \mathbb{Z}$  for which  $\gcd(a, b) = ak + b\ell$ .

## Example

#### **Proposition 7.1** If $a, b \in \mathbb{N}$ then

there exist  $k, \ell \in \mathbb{Z}$  for which  $gcd(a, b) = ak + b\ell$ .

*Proof.* Suppose  $a, b \in \mathbb{N}$ .

Consider the set  $A = \{ax + by : x, y \in \mathbb{Z}\}.$ 

A contains positive integers and 0.

Let  $d \in A$  be the smallest positive integer.

 $d = ak + b\ell$  for some  $k, \ell \in \mathbb{Z}$ .

We will show that  $d = \gcd(a, b)$ .

First, prove that  $d \mid a$  and  $d \mid b$ .

Then show that it is the largest such number.