EXISTENCE PROOFS AND EQUIVALENCES

1. Let $a, b \in \mathbb{N}$. Our goal is to prove that a and b have a unique greatest common divisor. More precisely, we'll show that there is a unique integer d such that d divides both a and b and if c is an integer that also divides both a and b, then $c \leq d$. In mathematics:

$$\exists! d \in \mathbb{Z},\ d|a \wedge d|b \wedge \big(\forall c \in \mathbb{Z},\ (c|a \wedge c|b) \implies c \leq d\big)$$

Proof. Let $a, b \in \mathbb{N}$. Let $A = \{x \in \mathbb{Z} : x|a \text{ and } x|b\}$. If $n \in A$, then $n|a$, and thus $n \leq a$. It follows that if A has any elements at all, then it has a greatest element.

a) Prove that $A \neq \emptyset$.

b) Let d be the greatest element of A. Prove that $d = \gcd(a, b)$.

c) Now we prove that d is unique. Suppose that d' is an integer that divides both a and b and that d' is greater than or equal to all other divisors of both a and b. Show that $d' = d$.

□

Date: October 12, 2018.

Theorem 1. *Let $a \in \mathbb{Z}$. The following are equivalent:*

(1) a is even;
(2) $a - 1$ and $a + 1$ are both odd;
(3) $a^2 - 1$ is odd.

2. Prove Theorem 1 by showing that $1 \implies 2 \implies 3 \implies 1$.