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 $A \neq \emptyset$.

Solution. Observe that $1|a$ and $1|b$ regardless of the actual values of a and b. Hence $1 \in A$. Therefore $A \neq \emptyset$.

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

Solution. Because $d \in A$, we know that $d|a$ and $d|b$, so d is a common divisor of a and b. Also, if $c|a$ and $c|b$, then $c \in A$, so $c \leq d$. Therefore d is a greatest common divisor of a and 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 $d' = d$.

Solution. Because d is a divisor of both a and b, it follows that $d' \geq d$. In addition, $d'|a$ and $d'|b$, so $d' \in A$. Thus $d \geq d'$. The only way both inequalities can hold is if $d = d'$. Therefore there is only one greatest common divisor.

$\square$

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 $1 \implies 2 \implies 3 \implies 1$.

Solution. Let $a \in \mathbb{Z}$.

($1 \implies 2$). Suppose a is even. By definition $a = 2n$ for some $n \in \mathbb{Z}$. Hence $a + 1 = 2n + 1$, which is odd by definition. It also follows that $a - 1 = 2n - 1 = 2(n - 1) + 1$, which is also odd. Therefore both $a + 1$ and $a - 1$ are odd.

($2 \implies 3$). Suppose $a + 1$ and $a - 1$ are both odd. We know that the product of two odd numbers is again odd. Therefore $(a - 1)(a + 1) = a^2 - 1$ is odd.

($3 \implies 1$). We prove the contrapositive: if a is odd, then $a^2 - 1$ is even. Suppose a is odd. By definition there is an integer n such that $a = 2n + 1$. Then

$$\begin{aligned} a^2 - 1 &= (2n + 1)^2 - 1 \\ &= 4n^2 + 4n + 1 - 1 \\ &= 2(2n^2 + 2n). \end{aligned}$$

Therefore $a^2 - 1$ is even.

Date: October 12, 2018.