PROOFS I

Definition. Let $a, b \in \mathbb{Z}$.

a) a is **even** if there is $c \in \mathbb{Z}$ such that $a = 2c$. (This is the same as $2|a$).
b) a is **odd** if there is $c \in \mathbb{Z}$ such that $a = 2c + 1$.
c) a **divides** b, written $a|b$, if there is $c \in \mathbb{Z}$ such that $ac = b$. (Also expressed "b is divisible by a").
d) The **greatest common divisor** of a and b, written $\gcd(a, b)$, is the largest integer that divides both a and b.
e) The **least common multiple** of a and b, written $\operatorname{lcm}(a, b)$, is the smallest positive integer divisible by both a and b.

Definition. Let $n \in \mathbb{N}$.

a) If $n \geq 2$ and the only positive divisors n are 1 and n, then n is **prime**.
b) If $n \geq 2$ and n is not prime, then n is **composite**.[1]

Facts. We assume (without proof) the following:

a) If m and n are integers, then $m + n$, $m - n$, and mn are all integers.
b) Given integers m and n with $n > 0$, there are unique integers q and r such that $m = qn + r$ and $0 \leq r < n$.

Example. Let $a, b, c \in \mathbb{Z}$. Prove that if $a|b$ and $a|c$, then $a|(b + c)$.

Proof. Let $a, b, c \in \mathbb{Z}$ and suppose $a|b$ and $a|c$. By definition (of divides), there are integers m and n such that $am = b$ and $an = c$. It follows that $b + c = am + an = a(m + n)$. since $m + n$ is an integer, we see that $a|(b + c)$ (again by definition of divides). $\square$

1. Let $k, m, n \in \mathbb{Z}$. Prove that if $k|m$ and $k|(m + n)$, then $k|n$.

Date: September 20–22, 2021.

[1] 1 is neither prime nor composite.

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

a) Prove that if a is even, then a^2 is even.

b) State the converse of the the statement in part a. Is the converse true or false?

c) Can you prove the converse?

3. Let $m, n \in \mathbb{Z}$. Our goal is to prove that if either m or n is even, then mn is even.[2]

a) Write the contrapositive of the statement. Note that the contrapositive has the same implicit quantifiers as the original statement.

b) Since any statement is logically equivalent to its contrapositive, proving either one suffices to prove both. Which do you think will be easier?

c) Prove that if m is even, then mn is even.

d) Is this enough to prove if either m or n is even, then mn is even?

Challenge (write your solution on a separate sheet of paper)**.** Prove that if $n \in \mathbb{N}$ and $n \geq 2$, then the numbers $n! + 2$, $n! + 3$, $n! + 4$, $\ldots$, $n! + n$ are all composite. (This means that $n! + 2$, $n! + 3$, $n! + 4$, $\ldots$, $n! + n$ is a sequence of $n - 1$ consecutive composite numbers, thus showing that there are arbitrarily large gaps between prime numbers).

[2]This should be easy, right?