Not Euler's

Euclid's Lemma: Suppose $a, b \in \mathbb{Z}$ and p is prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

If a number divides a product, must it divide one of the factors?

$3 \mid 18$

$18 = 6 \cdot 3$ $3 \mid 6$ and $3 \mid 3$

$18 = 2 \cdot 9$ $3 \mid 9$

$18 = 1 \cdot 18$ $3 \mid 18$

$6 \mid 24$

$24 = 2 \cdot 12$ $6 \mid 12$

$24 = 3 \cdot 8$ $6 \nmid 3$, $6 \nmid 8$!

$9 \mid 90$ ✓

$90 = 9 \cdot 10$ $9 \mid 9$

$90 = 45 \cdot 2$ $9 \mid 45$

$90 = 6 \cdot 15$ ✗

$90 = 3 \cdot 30$ ✗

If and only if - biconditionals

$P \longleftrightarrow Q$ "P if and only if Q"

means: $(P \rightarrow Q) \wedge (Q \rightarrow P)$

Outline - proofs of if and only if statements

Prop. $P \longleftrightarrow Q$

Proof.

"Forwards direction"

(First, prove $P \rightarrow Q$, using direct, contrapositive, or contradiction) "backwards direction"

Conversely,
(Then prove $Q \to P$, using direct, contrapositive, or contradiction)
$\square$

given $P \to Q$, we call $Q \to P$ the converse of the original.
Use "conversely" to introduce the second part.

Ex

Prop an integer n is even $\underbrace{\text{if and only if}}_{\text{"iff"}}$ n^2 is even.

Proof (forwards direction) (Direct): Suppose $n \in \mathbb{Z}$ is even.
then $n = 2b$, $b \in \mathbb{Z}$, by definition of even.
so $n^2 = (2b)^2 = 4 \cdot b^2 = 2(2b^2)$
Note $2b^2 \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under $\cdot$

Thus n^2 is even, by the definition of even.

"if n^2 is even then n is even"
lets use contrapositive.
"if n is ~~not even~~ odd then n^2 is ~~not even~~ odd"

Conversely, suppose $n \in \mathbb{Z}$ is odd.
Then $n = 2c+1$, $c \in \mathbb{Z}$ by definition of odd.

$$n^2 = (2c+1)^2 = (2c+1)(2c+1)$$
$$= 4c^2 + 2c + 2c + 1$$
$$n^2 = \underbrace{4c^2 + 4c} + 1$$
$$n^2 = 2(2c^2 + 2c) + 1$$

Then $2c^2 + 2c \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under multiplication and addition.
Thus n^2 is odd, by the definition of odd.

$\square$

$A \to B$
contrapositive:
Suppose $\sim B$.
⋮
Thus $\sim A$.

Existence proofs

Prop $\exists x\, P(x)$

Proof: (give an example of such an x, show it satisfies $P(x)$)

Prop. There exists an even prime number.

Proof. Consider the number 2. It is even, and it is also prime. $\square$

Prop There exists a natural number n such that $n^2 - 2 = 7$.

Proof. Suppose $n = 3$. Then $n \in \mathbb{N}$, and $n^2 - 2 = 3^2 - 2 = 9 - 2 = 7$.

Prop There is an integer that can be expressed as the sum of two cubes in two different ways.

Proof Consider the number 1729. Notice $1729 \in \mathbb{Z}$.

Note that
$$1^3 + 12^3 = 1729 \text{ and}$$
$$9^3 + 10^3 = 1729.$$
$\square$

$3^3 + 1^3 =$

$27 + 1 = 28$

$28 \in \mathbb{Z}$

$28 = 3^3 + 1^3$

$X = \boxed{}\,?$

$35 = 3^3 + 2^3$

1729

$1 + 1728$

$1^3 + 12^3 = 1729$

$\boxed{\text{Ramanujan}}$

$9^3 + 10^3$

$729 + 1000 = 1729$

Prop Suppose $a \in \mathbb{Z}$. Then $6|a$ if and only if $2|a$ and $3|a$.

Proof ($\rightarrow$) Suppose $a \in \mathbb{Z}$ and $6|a$.

So $a = 6b$, $b \in \mathbb{Z}$ by defn of divides.

$a = 2 \cdot 3 \cdot b$

$6|6$

$2|6$ and $3|6$?

$6|18$

$2|18$ ✓

$a = 2(3b)$

Note $3b \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under multiplication

so $2|a$ by defn of divides

also $a = 3(2b)$

and $2b \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under multiplication.

thus $3|a$ by definition of divides.

Thus $2|a$ and $3|a$

$2|18$ ✓

$3|18$ ✓

$6|-18$

then

$2|-18$

and

$3|-18$

Conversely, (direct proof) Suppose $a \in \mathbb{Z}$ and $2|a$ and $3|a$.

Then $a = 2x$ for some $x \in \mathbb{Z}$ and ~~$a = 3y$ for some $y \in \mathbb{Z}$~~ by definition of divides.

not needed.

Since $3|a$ and $a = 2x$, we have $3|2x$.

Since 3 is prime and $2x \in \mathbb{Z}$, Since 3 is prime and ... by

Euclids Lemma tells us that either $3 \mid 2$ or $3 \mid x$

Since $3 \nmid 2$, we must have $3 \mid x$.

So $x = 3 \cdot c$, $c \in \mathbb{Z}$ by definition of divides

$a = 2x = 2 \cdot 3 \cdot c$

$a = 6 \cdot c$, $c \in \mathbb{Z}$.

Thus $6 \mid a$, by definition of divides

$\square$