Alison Li

Problem.
Write the theorem: "Every integer is either even or odd" in symbolic logic using only the '$\equiv$' predicate.

$\forall n \in \mathbb{Z}$ (n is even $\vee$ n is odd).

$\forall n \in \mathbb{Z}$ $[\exists m \in \mathbb{Z}\ n = 2m) \vee (\exists \ell \in \mathbb{Z}\ \ n = 2\ell + 1)$.

Multiple Quantifiers

If you have a '$\forall$' and an '$\exists$', the order matters.

Examples:

(1) $\forall x \in \mathbb{R}\ \ \exists y \in \mathbb{R}\ \ x + y = 0$.
True. Set $y = -x$.

(2) $\exists y \in \mathbb{R}\ \ \forall x \in \mathbb{R}\ \ x + y = 0$.
False. There is no fixed y for any x.

(3) $\exists y \in \mathbb{R}\ \ \forall x \in \mathbb{R}\ \ xy = 0$.
True, since for $y = 0$, for any x, $x(0) = 0$.

(4) $\forall x \in \mathbb{R}\ \ \exists y \in \mathbb{R}\ \ xy = 0$.
True. You can always set $y = 0$.

If you have several '$\forall$' or '$\exists$', order doesn't matter.

ex. $\forall x \in \mathbb{R}\ \ \forall y \in \mathbb{R}\ \ x^2 + y^2 \geq 0$ is the same as:
$\forall y \in \mathbb{R}\ \ \forall x \in \mathbb{R}\ \ x^2 + y^2 \geq 0$
$\forall x, y \in \mathbb{R}\ \ x^2 + y^2 \geq 0$

def. Let $m, n \in \mathbb{Z}$. We say m divides n (m is a factor of n) if $m \neq 0$ and $n = m\ell$ for some $\ell \in \mathbb{Z}$). Denoted as $m | n$.

ex. $2 | 10$ since $10 = 2 \cdot 5$ and $2 \neq 0$.

We can define the predicate "$m|n$" as follows:
$\forall m, n \in \mathbb{Z}\ [m|n \Leftrightarrow (\neg(m=0) \wedge \exists \ell \in \mathbb{Z}\ \ n = m\ell)]$.

def. $n \in \mathbb{N}$ is prime if $n \geq 2$ and only divisors of n are 1 and n.

Problem.
Define predicate $P(n)$, "n is prime", in symbolic logic.

$\forall n \in \mathbb{N}\ \ [P(n) \Leftrightarrow (n \geq 2 \wedge ($if $m|n$ then $m = 1$ or $m = n)]$

$\forall n \in \mathbb{N}\ \ [P(n) \Leftrightarrow (n \geq 2 \wedge (\forall m \in \mathbb{N}\ (m|n \Rightarrow m = 1 \vee m = n)]$

Negating Quantifiers

Let $Q(x)$ be any predicate. Then,

$\neg \forall n\ \ Q(n) \equiv \exists n\ \ \neg Q(n)$.

$\neg \exists n\ \ Q(n) \equiv \forall n\ \ \neg Q(n)$.

Alison Li

ex. Negate $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R}\ x+y=0$.
Formally,

$$\neg(\exists x\ \forall y\ x+y=0) \equiv \forall x\ \neg\forall y\ x+y=0$$
$$\equiv \forall x\ \exists y\ \neg(x+y=0)$$
$$\equiv \forall x\ \exists y\ x+y\neq 0.$$

ex. Define "n is not prime" by negating definition of prime.

$\forall n \in (\neg P(n) \Leftrightarrow \neg(n \geq 2 \wedge (\forall m \in \mathbb{N}\ (m|n \Rightarrow m=1 \vee m=n))$

Simplify:

$\neg(n \geq 2 \wedge (\forall m \in \mathbb{N}\ (m|n \Rightarrow m=1 \vee m=n))$
$\equiv \neg(n \geq 2) \vee \neg(\forall m\ (m|n \Rightarrow m=1 \vee m=n))$ by de Morgan
$\equiv (n<2) \vee (\exists m\ \neg(m|n \Rightarrow m=1 \vee m=n))$
$\equiv (n<2) \vee (\exists m\ \neg(\neg(m|n) \vee m=1 \vee m=n)))$
$\equiv (n<2) \vee (\exists m\ (m|n) \wedge m\neq 1 \wedge m\neq n)$

Hence,

$\forall n\ [\neg P(n) \Leftrightarrow (n<2 \vee \exists m\ (m|n \wedge m\neq 1 \wedge m\neq n)]$.

Proofs

To prove $\exists x\ Q(x)$: Find a specific x that works, i.e. for which $Q(x)$ is true.

ex. Prove $\exists m,n \in \mathbb{N}\ (m^2+n^2=25 \wedge m\neq 0 \wedge n\neq 0)$.
proof. Set $m=3$, $n=4$. Then, $m\neq 0$, $n\neq 0$, and $3^2+4^2=25$. □

To prove $\forall x \in U\ Q(x)$: You need to prove $Q(x)$ true for an arbitrary element of U. Say "let $x \in U$", then show $Q(x)$ true for this x.

ex. Set $A=\{n \in \mathbb{N} \mid \exists m \in \mathbb{N}\ n=2m+1\}$ (odd natural numbers).
Prove $\forall n \in A,\ 2|(n+1)$.

proof.
Let $n \in A$. Since $n \in A$, we know $\exists m\ n=2m+1$.
Then, $n+1=(2m+1)+1=2m+2=2(m+1)$.
So, since $2\neq 0$ and $n+1=2\ell$ for $\ell=m+1 \in \mathbb{Z}$, $2|(n+1)$.
Hence, $\forall n \in A\ 2|(n+1)$. □

To prove $P \Rightarrow Q$: assume P is true, then use this information to prove Q is true.

ex. Prove $\forall a,b,c \in \mathbb{Z}\ (a|b \wedge b|c) \Rightarrow (a|c)$.

proof.
Let $a,b,c \in \mathbb{Z}$. Assume $a|b$ and $b|c$.
Since $a|b$, $a\neq 0$ and $b=an$ for some $n \in \mathbb{Z}$.
Since $b|c$, $b\neq 0$ and $c=bm$ for some $m \in \mathbb{Z}$.
Then, $c=bm=(an)m=a(nm)=a\ell$, where $\ell=nm$.

Alison Li

So, $a \neq 0$ and $c = a\ell$, where $\ell \in \mathbb{Z}$ since $m, n \in \mathbb{Z}$.
Hence, $a \mid c$. $\square$