Test 1

1. a. $\quad L \Rightarrow R$

$$[(C \Rightarrow A) \Rightarrow (A \wedge B \wedge \neg C \wedge D)] \Rightarrow [B \wedge D \wedge ((A \Rightarrow C) \Rightarrow \neg(C \Rightarrow A))]$$

Assume L is True.

Case 1: $C \Rightarrow A$ is False

Case 2: $C \Rightarrow A$ is True and $A \wedge B \wedge \neg C \wedge D$ is True

Case 1

C must be True and A must be False so $A \wedge B \wedge \neg C \wedge D$ is False because A is False. On the right, $((A \Rightarrow C) \Rightarrow \neg(C \Rightarrow A)) \Leftrightarrow (\text{True} \Rightarrow \text{True})$. R becomes $B \wedge D \wedge \text{True}$. If either B or D are False, then $L \Rightarrow R$ is False $\blacksquare$

b. $\quad R \Rightarrow L$

$$[B \wedge D \wedge ((A \Rightarrow C) \Rightarrow \neg(C \Rightarrow A))] \Rightarrow [(C \Rightarrow A) \Rightarrow (A \wedge B \wedge \neg C \wedge D)]$$

Assume that R is True. This means the B and D are True and that A and C are not equal (A True, C False or A False, C True). Then, L is False when $C \Rightarrow A$ is True and $A \wedge B \wedge \neg C \wedge D$ is False. However, in order for $C \Rightarrow A$ to be True, C must be False and A must be True, so $A \wedge B \wedge \neg C \wedge D$ is True. Therefore, $R \Rightarrow L$ is True. $\blacksquare$

2. L: There is a unique element in S with property P.

R: $\exists (x \in S) : (P(x) \wedge \forall (y \in S) : P(y) \Rightarrow x = y))$

$L \Leftrightarrow R$

Prove $L \Rightarrow R$:

First, assume L is True.
Let x be a unique element in S such that $P(x)$.
Since x is unique, there is only one of x in S.
Assume $P(y)$ is True. Since there is only one element with property P, y is just an alias of x so $y = x$ and R has to be True. $\blacksquare$

Prove $R \Rightarrow L$:

Assume $\neg L$ so there isn't a unique element in S with property P. There are two cases here: either there doesn't exist an element with property P or there exists more than one element with property P. This can be written as $\forall (x \in S) : (\neg P(x) \vee \exists (y \in S) : P(y) \wedge x \neq y)$, which is just $\neg R$ so $\neg R$ is True. $\blacksquare$

3. Property: $\forall (B \in \mathbb{R}) \exists (C \in \mathbb{R}) \forall (x \geq C) : f(x) \geq B$
If $f(x) = -x^2$, it doesn't satisfy this property. Because $f(x) = -x^2$, $f(x)$ is always ≤ 0. If a B is chosen that is greater than 0, there is no x that makes $f(x) \geq B$. $\blacksquare$

4. $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ $\quad f_b(x) = bx + 1 \pmod{n}$

f_b is bijective $\iff \gcd(b, n) = 1$

Prove: f_b is bijective $\Rightarrow \gcd(b,n) = 1$

Assume $\gcd(b,n) \neq 1$, so $\gcd(b,n) > 1$.
Let $\gcd(b,n)$ be k. Let $b = ki$ and $n = kj$. $f_b(x) = kix + 1 \pmod{kj}$. Since b and n are not relatively prime, there exists x_1 and x_2 where $x_1 \neq x_2$ and $f_b(x_1) = f_b(x_2)$. This means that f_b is not injective. ∎

Prove: $\gcd(b,n) = 1 \Rightarrow f_b$ is bijective

Assume that f_b is not bijective, so f_b is either not surjective or not injective.
When f_b is not injective, this means there exists x_1 and x_2 where $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$.
$f_b(x_1) = bx_1 + 1 \pmod n = f_b(x_2) = bx_2 + 1 \pmod n$.

$bx_1 + 1 \equiv bx_2 + 1 \pmod n$

$(bx_1 + 1) - (bx_2 + 1) = kn$ for some $k \in \mathbb{Z} = b(x_1 - x_2)$

This means there is some common factor between b and n greater than 1 so $\gcd(b,n) \neq 1$. ∎

EC. The kingfisher travels in a combination of vertical and horizontal movements. Going diagonally compared to going linearly doesn't matter as the perimeter is equivalent.

Prove: move to (m, n) in ℓ hops iff

$\ell \geq |m| + |n|$ and $\ell \equiv m+n \pmod 2$

Assume it can move to (m,n) in ℓ hops and $\ell < |m|+|n|$ or $\ell \not\equiv m+n \pmod 2$.

$\ell < |m|+|n|$ because $|m|+|n|$ is its shortest Manhattan distance.

Base case: (m,n) is $(0,0)$

ℓ can't be < 0 because can't be negative hops so $\ell < |m|+|n|$ is always False. Let $\ell = 0$ since that is the min. number of hops.

$0 \equiv (0+0) \pmod 2$. Contradiction.

Assume $\ell \geq |m|+|n|$ and $\ell \equiv m+n \pmod 2$.

One way to get to (m,n) is to move m times in the x direction and move n times in the y direction. Therefore, it can move to (m,n) in ℓ hops.