How (not) to prove that a function $f : A \to B$ is onto

Suppose f is a function from A to B, and suppose we pick some element $a \in A$ and some element $b \in B$. If $f(a) = b$ then we say that b is **the image** of a (under f), and we say that a is **a pre-image** of b (under f). I'll omit the "under f" from now. Try to understand each of the following four items:

1. No matter how you choose a, it always has **one image** (namely $f(a)$).
2. If f is not onto, then there is some b in B that does not have a pre-image.
3. If f is not 1-1, then there is some b in B with more than one pre-image.
4. Can you see why I used ***the*** image, and ***a*** pre-image? (***the image*** because of item 1, and ***a pre-image*** because of items 2,3).

If any of 1–4 is not clear, please ask.

Now fix some element $b \in B$.

(1) The statement "b has a pre-image" is the same as $\exists_{a \in A}\ f(a) = b$.
(2) The statement "a is a pre-image of b" is the same as $f(a) = b$.

Consider the two statements: (1): $\exists_{a \in A}\ f(a) = b$, and (2): $f(a) = b$. Are statements (1),(2) the same? (they are treated the same in many of your proofs…)

Statement (1) only says that b has a pre-image.
Statement (2) says more: It says that a is a pre-image of b.

Do you see the difference? Saying (1): "problem P has a solution" isn't the same thing as saying (2) "a is a solution of P".

Saying that a problem has a solution is not the same thing as saying that the element $a \in A$ we happened to pick is a solution of P. So we should always be careful with quantifiers $\forall$ and $\exists$ (if we use words instead of these symbols, the same care is still needed!). We can not simply add or drop these quantifiers whenever we want, there are rules for that.

With all of that in mind, lets look at a bad (but unfortunately, very common) way to prove something. As an example, lets take $A = \{-2, -1, 0, 1, 2\}$ and $B = \{0, 1, 2, 3, 4\}$ and the function $f : A \to B$ is the function that sends x to x^2. Consider the statement S: "f is onto" and lets either prove or disprove S. Statement S says this:

S: Every $b \in B$ has a pre-image (under f)
S: $\forall_{b \in B} \exists_{a \in A}\ f(a) = b$

Bad Proof: For each $a \in A$: lets compute $f(a) = a^2$ and then take $b = f(a)$. Lo and behold, each b in B we encountered has a pre-image! Hence S is true.

If that was a valid proof then many of would have had more points.

If we want to check that if f is onto, it is **not enough** to take elements of A, take their images in B, and then check that those images have pre-images!

How to prove that a function is onto

Checking that f is onto means that we have to check that **all elements** of B have a pre-image. It is not enough to check only those $b \in B$ that we happen to run into. Going back to the example, we have to allow b to be any element of B. So b could be 0 (has a pre-image), or b could be 1 (has a pre-image) or b could 2 (has no pre-image!) That means we proved $\neg S$, in other words, f is not onto. (what about $b = 3$? Doesn't $b = 3$ also prove that f is not onto? Yes, but there's no point in proving $\neg S$ twice).

In the quiz you are asked to prove that $g \circ f : A \to C$ is onto. Do not start your proof by saying that $g(f(a)) = c$ or that $f(a) = b$ because if you do that, how would your proof be different from the Bad Proof on page 1?

To ensure our proof covers every $c \in C$, we can not start with some a in A or some $b \in B$ and then compute c from it, because that is what "Bad Proof" on page 1 did. To ensure we cover any c in C, we start with any c in C, and then the other letters (a or b) come after c is already fixed. So lets look at the question one more time:

Let $f : A \to B$ and $g : B \to C$ and suppose both are onto. Prove that the composition $g \circ f : A \to C$ is onto.

L1. Given: (G1) $\forall_{c \in C} \exists_{b \in B}\ g(b) = c$.
L2. Given: (G2) $\forall_{b \in B} \exists_{a \in A}\ f(a) = b$.
L3. To prove: $\forall_{c \in C} \exists_{a \in A}\ g(f(a)) = c$.
L4. Let $c \in C$. (Notice that "Bad Proof" did not start this way!)
L5. To prove: $\exists_{a \in A}\ g(f(a)) = c$.
...

What do we need to prove?
(1): $\exists_{a \in A}\ g(f(a)) = c$, or
(2): $g(f(a)) = c$.
As explained on page 1, that is not the same thing.

Statement (1) says: $g(f(a)) = c$ *for some a in A.*
Statement (2) says: $g(f(a)) = c$ *without any indication what a is!*

But if we have no indication what a is, then it's simply not possible to prove that $g(f(a)) = c$. If a could be anything, then $g(f(a))$ could be something totally different than c. So statement (2) can not be proven (so do not attempt that). We have to prove statement (1).

When using statement (G2) it is important to understand that:

(G2) **does not say** that $f(a)$ is equal to b.

(G2) only says (about any b in B) that $f(a)$ is equal to b **for some** a **in** A.

But if you already picked some $a \in A$ then (G2) **does not say** that $f(a) = b$.