The result? The question is whether we have only *one* result to justify the article "the". We summarize telegrammaticaly. To find $X \bigoplus Y$,

1)choose a $\in \mathbb{Z}$ from X,

2)choose b $\in \mathbb{Z}$ from Y,

3)find $a+b$ in $\mathbb{Z}$,

4)take the residue class of $a+b$.

This sounds a perfectly good recipe for finding $X \bigoplus Y$ but notice that we use some auxiliary objects, namely a and b, to find $X \bigoplus Y$, which must be determined by X and Y alone. Indeed, the result $\overline{a+b}$ depends explicitly on the auxiliary objects a and b. We can use our recipe with different auxiliary objects. Let us do it. 1) I choose a from $X \subseteq \mathbb{Z}$ and you choose a_1 from X. 2) I choose b from $Y \subseteq \mathbb{Z}$ and you choose b_1 from Y. 3) I compute $a+b$ and you compute a_1+b_1. In general, $a+b \neq a_1+b_1$. Hence our recipe gives, generally speaking, distinct elements $a+b$ and a_1+b_1. So far, both of us followed the same recipe. I cannot claim that my computation is correct and yours is false. Nor can you claim the contrary. Now we carry out the fourth step. I find the residue class of $a+b$ as $X \bigoplus Y$, and you find the residue class of a_1+b_1 as $X \bigoplus Y$. Since $a+b \neq a_1+b_1$ in $\mathbb{Z}$, it can very well happen that $\overline{a+b} \neq \overline{a_1+b_1}$ in $\mathbb{Z}_n$. On the other hand, if $\bigoplus$ is to be a binary operation on $\mathbb{Z}_n$, we must have $\overline{a+b} = \overline{a_1+b_1}$ whenever $\overline{a} = \overline{a}_1, \overline{b}_1 = \overline{b}$, even if $a+b \neq a_1+b_1$. If there is such a mechanism, we say $\bigoplus$ is a well defined operation on $\mathbb{Z}_n$. This means $\bigoplus$ is really a genuine operation on $\mathbb{Z}_n : X \bigoplus Y$ is uniquely determined by X and Y alone. Any dependance of $X \bigoplus Y$ on auxiliary integers $a \in X$ and $ba \in Y$ is only apparent. We will prove that $\bigoplus$ and $\bigotimes$ are well defined operation on $\mathbb{Z}_n$, but before that, we discuss more generally well definition of functions.

A function $f : A \to B$ is essentialy a rule by which each element a of A is associated with a unique element of $f(a) = b$ of B. The important point is that the rule produces an element $f(a)$ that depends only on a. Sometimes we consider rules having the following form. To find $f(a)$,

1)do this and that

2)take an x related a in such and such manner

3)do this and that to x

4)the result is $f(a)$.