and *b)*. 2) Evaluate $F(a)$ and $F(b)$. 3) Put $I(f) = F(b) - F(a)$. There are many functions F with $F'(x) = f(x)$ for all $x \in [a, b]$. For two different choices F_1 and F_2, we have $F_1(b) \neq F_2(b)$ and $F_1(a) \neq F_2(a)$ in general. So we may suspect that $F_1(b) - F_1(a) \neq F_2(b) - F_2(a)$. In order to show that I is a well defined function, we must prove $F_1(b) - F_1(a) = F_2(b) - F_2(a)$ whenever F_1 and F_2 are functions on $[a, b]$ such that $F_1'(x) = f(x) = F_2'(x)$ for all $x \in [a, b]$. We know from the calculus that, when F_1 and F_2 have this property, there is a constant c such that $F_1(x) = F_2(x) + c$ for all $x \in [a, b]$. So $F_1(b) - F_1(a) = (F_2(b) + c) - (F_2(a) + c) = F_2(b) - F_2(a)$. Therefore, I is well defined.

After this lengthy digression, we return to the integers mod n and to the "operations" $\bigoplus$ and $\bigotimes$.

Lemma 0.1. *$\bigoplus$ and $\bigotimes$ are well defined operations on $\mathbb{Z}_n$*

Proof. We are to prove $\bar{a} \bigoplus \bar{b} = \bar{a}' \bigoplus \bar{b}'$ whenever $\bar{a} = \bar{a}'$ and $\bar{b} = \bar{b}'$ in $\mathbb{Z}_n$ (different names for identical residue classes should not yield different results.) This follows from *Lemma 6.1*. Indeed, if $\bar{a} = \bar{a}'$ and $\bar{b} = \bar{b}'$, then $a \equiv a'(mod n)$ and $b \equiv b'(\text{mod } n)$ by definition, so we obtain $a + b = a' + b'(\text{mod } n)$ and $ab = a'b'(\text{mod } n)$ by *Lemma 6.1*, hence $\overline{a + b} = \overline{a' + b'}$ and $\overline{ab} = \overline{a'b'}$, which gives $\bar{a} \bigoplus \bar{b} = \overline{a + b} = \overline{a' + b'} = \bar{a}' \bigoplus \bar{b}'$ and $\bar{a} \bigotimes \bar{b} = \overline{ab} = \overline{a'b'} = \bar{a}' \bigotimes \bar{b}'$. □

Having proved that $\bigoplus$ and $\bigotimes$ are well defined operations on $\mathbb{Z}_n$, we proceed to show that $\bigoplus$ and $\bigotimes$ possess many (but not all) properties of the usual addition ad multiplication of integers. First we simplify our notation. From now on, we write $+$ and . instead of $\bigoplus$ and $\bigotimes$. In fact, we shall even drop and use simply juxtaposition to denote a product of two integers mod n. Thus we will have $\bar{a} + \bar{b} = \overline{a + b}$ and $\bar{a} \,.\, \bar{b} = \overline{ab}$ or simply $\bar{a}\ \bar{b} = \overline{ab}$. The reader should note that the same sign "+" is used to denote two very distinct operations: $\bigoplus$ in the old notation and the usual addition of integers. If anything, they are defined on distinct sets $\mathbb{Z}_n$ and $\mathbb{Z}$. The same remarks apply to multiplication.