Multiplication on the Integers

$\mathbb{Z} = \{[(a,b)]_\sim \mid a,b \in \mathbb{N}\}$

$\hookrightarrow$ "a−b"

$(a,b) \sim (c,d) \iff a+d = c+b$

$[(a,b)]_\sim + [(c,d)]_\sim = [(a+c, b+d)]_\sim$

"a−b" "c−d" "(a+c)−(b+d)"

Definition

$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac+bd, ad+bc)]$

"a−b" "c−d" "(a−b)(c−d)" = "ac−ad−bc+bd"

= "(ac+bd)−(ad+bc)"

Proposition:

(1) $\cdot$ is commutative on $\mathbb{Z}$

Proof: show that $[(a,b)]_\sim \cdot [(c,d)]_\sim = [(c,d)]_\sim \cdot [(a,b)]_\sim$

$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac+bd, ad+bc)]_\sim$ by definition

$= [(ca+db, da+cb)]_\sim$ comm of $\cdot \mathbb{N}$

$= [(ca+db, cb+da)]_\sim$ comm of $+\mathbb{N}$

$= [(c,d)]_\sim \cdot [(a,b)]_\sim$ by definition

(2) $\cdot_{\mathbb{Z}}$ is associative

Proof: show that $([(a,b)]_\sim \cdot [(c,d)]_\sim) \cdot [(e,f)]_\sim = [(a,b)]_\sim \cdot ([(c,d)]_\sim \cdot [(e,f)]_\sim)$

from starting point:

$([(a,b)]_\sim \cdot [(c,d)]_\sim) \cdot [(e,f)]_\sim = [(ac+bd, ad+bc)]_\sim \cdot [(e,f)]_\sim$

$= [((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e)]_\sim$

$= [(ace+bde+adf+bcf, acf+bdf+ade+bce)]_\sim$

from ending point

$[(a,b)]_\sim \cdot ([(c,d)]_\sim \cdot [(e,f)]_\sim) = [(a,b)]_\sim \cdot [(ce+df, cf+de)]_\sim$

$= [(a(ce+df)+b(cf+de), a(cf+de)+b(ce+df))]_\sim$

$= [(ace+adf+bcf+bde, acf+ade+bce+bdf)]_\sim$

these endpoints are equal to each other

$\therefore$ $\cdot_{\mathbb{Z}}$ is associative.

(3) for all $x,y,z \in \mathbb{Z}$, $x\cdot(y+z) = (x+y)+(x+z)$ left distributive law

Proof: let $x = [(a,b)]_\sim$ $y = [(c,d)]_\sim$ & $z = [(e,f)]_\sim$

from start forward

$x\cdot(y+z) = [(a,b)]_\sim \cdot [(c+e, d+f)]$

$= [(a(c+e)+b(d+f), a(d+f)+b(c+e))]_\sim$

from end backward

$x\cdot y + x\cdot z = [(ac+bd, ad+bc)]_\sim + [(ae+bf, af+be)]_\sim$

$= [(ac+bd+ae+bf, ad+bc+af+be)]_\sim$

with some factoring, these are equal

Rules

Given:

1. $0_{\mathbb{Z}} = [(0,0)]_\sim = \{(a,b) \mid a=b\}$
2. $1_{\mathbb{Z}} = [(1,0)]_\sim = \{(a,b) \mid a = S(b)\}$

$\Rightarrow$ for all $z \in \mathbb{Z}$, $z \cdot 0_{\mathbb{Z}} = 0_{\mathbb{Z}}$ & $z \cdot 1_{\mathbb{Z}} = z$

$\Rightarrow$ $-[(a,b)]_\sim = [(b,a)]_\sim$

$\Rightarrow$ $z + (-z) = 0_{\mathbb{Z}}$

Given: $\phi: \mathbb{N} \to \mathbb{Z}$

$\Rightarrow$ $\phi(n) = [(n,0)]_\sim$

$\Rightarrow$ ϕ is 1-1 & $\phi(n+k) = \phi(n) + \phi(k)$

$\phi(nk) = \phi(n)\phi(k)$

$\phi(0_{\mathbb{N}}) = 0_{\mathbb{Z}}$

$\phi(1_{\mathbb{N}}) = 1_{\mathbb{Z}}$