MA 1101 : Mathematics I

Satvik Saha, 19MS154 September 29, 2019

1 Integers

Theorem 1.1. *Define a relation $\sim_{\mathbb{Z}}$ on $\mathbb{N} \times \mathbb{N}$ as*

$$(m, n) \sim_{\mathbb{Z}} (p, q) \quad \textit{if} \quad m + q = n + p.$$

Then, $\sim_{\mathbb{Z}}$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

Proof. For an arbitrary $(m, n) \in \mathbb{N} \times \mathbb{N}$, clearly $(m, n) \sim_{\mathbb{Z}} (m, n)$, hence $\sim_{\mathbb{Z}}$ is reflexive.

Again, for arbitrary $(m, n), (p, q) \in \mathbb{N} \times \mathbb{N}$, if $(m, n) \sim_{\mathbb{Z}} (p, q)$, we have $m + q = n + p$. By the commutativity of addition on natural numbers, $p+n = q+m$, so $(p, q) \sim_{\mathbb{Z}} (m, n)$, hence $\sim_{\mathbb{Z}}$ is symmetric.

For $(m, n), (p, q), (r, s) \in \mathbb{N} \times \mathbb{N}$, if $(m, n) \sim_{\mathbb{Z}} (p, q)$ and $(p, q) \sim_{\mathbb{Z}} (r, s)$, we have $m + q = n + p$ and $p + s = q + r$. Thus, $m + q + p + s = n + p + q + r$, so $m + s = n + r$. Thus, $(m, n) \sim_{\mathbb{Z}} (r, s)$, hence $\sim_{\mathbb{Z}}$ is transitive.

Therefore, $\sim_{\mathbb{Z}}$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$. □

Notation. Let us set

$$\mathbb{Z} \;:=\; (\mathbb{N} \times \mathbb{N})/\sim_{\mathbb{Z}},$$

$$\mathbb{Z}^+ \;:=\; \{[(n + 1, 1)] : n \in \mathbb{N}\}, \quad \bar{0} \;:=\; [(1, 1)], \quad \bar{1} \;:=\; [(2, 1)].$$

Definition (Addition). For $a = [(m, n)],\ b = [(p, q)] \in \mathbb{Z}$, we define

$$a + b \;:=\; [(m + p, n + q)].$$

Theorem 1.2. *Addition $(+)$ is well-defined, associative and commutative.*

Proof. First, we show that $+$ is well-defined. Let $a = [(m, n)] = [(m', n')]$, $b = [(p, q)] = [(p', q')] \in \mathbb{Z}$. We claim that $a + b = [(m + p, n + q)] = [(m' + p', n' + q')]$, i.e. $(m + p, n + q) \sim_{\mathbb{Z}} (m' + p', n' + q')$, i.e $m + p + n' + q' = n + q + m' + p'$. Now, $(m, n) \sim_{\mathbb{Z}} (m', n')$ and $(p, q) \sim_{\mathbb{Z}} (p', q')$, from which we have $m + n' = n + m'$ and $p + q' = q + p'$. Adding these gives the desired result.

For $a, b, c \in \mathbb{Z}$, let $a = [(m, n)], b = [(p, q)], c = [(r, s)]$. From the associativity of addition in $\mathbb{N}$,

$$\begin{aligned}
(a + b) + c &= [(m + p, n + q)] + [(r, s)] \\
&= [((m + p) + r, (n + q) + s)] \\
&= [(m + (p + r), n + (q + s))] \\
&= [(m, n)] + [(p + r, q + s)] \\
&= a + (b + c)
\end{aligned}$$

Therefore, $+$ is associative.

From the commutativity of addition in $\mathbb{N}$,

$$\begin{aligned}
a + b &= [(m + p, n + q)] \\
&= [(p + m, q + n)] \\
&= b + a
\end{aligned}$$

Therefore, $+$ is commutative. □

Theorem 1.3. *For all $a \in \mathbb{Z}$, $\bar{0} + a = a = a + \bar{0}$.*

Proof. Let $a = [(m,n)] \in \mathbb{Z}$. Note that $(m,n) \sim_{\mathbb{Z}} (m+1, n+1)$.

$$\begin{aligned} a + \bar{0} &= [(m,n)] + [(1,1)] \\ &= [(m+1, n+1)] \\ &= [(m,n)] \\ &= a \\ a + \bar{0} &= a = \bar{0} + a \end{aligned}$$

□

Theorem 1.4. *For all $a \in \mathbb{Z}$, there exists a unique $x \in \mathbb{Z}$, satisfying $a + x = \bar{0} = x + a$.*

Proof. For $a = [m,n] \in \mathbb{Z}$, construct $x = [(n,m)] \in \mathbb{Z}$. Clearly, $a + x = [(m+n, n+m)] = \bar{0}$. From commutativity of $+$, $a + x = \bar{0} = x + a$.

We now show that x is unique. Let $a + x' = \bar{0} = x' + a$.

$$\begin{aligned} a + x' &= \bar{0} \\ x + (a + x') &= x + \bar{0} \\ (x + a) + x' &= x \\ \bar{0} + x' &= x \\ x' &= x \end{aligned}$$

□

Notation. We denote x as $-a$ and say that $-a$ is the *negative* of a.

For $a, b \in \mathbb{Z}$, we write

$$a - b := a + (-b).$$

Theorem 1.5. *For all $a, b \in \mathbb{Z}$, there exists a unique $x \in \mathbb{Z}$ satisfying $a + x = b$.*

Proof. For the well-defined nature of $+$, there exists a unique $x = b - a = b + (-a) \in \mathbb{Z}$.

$$\begin{aligned} a + x &= a + (b + (-a)) \\ &= a + ((-a) + b) \\ &= (a + (-a)) + b \\ &= \bar{0} + b \\ &= b \end{aligned}$$

□

Definition (Multiplication). For $a = [(m,n)],\ b = [(p,q)] \in \mathbb{Z}$, we define multiplication

$$a \cdot b := [(mp + nq, mq + np)].$$

Theorem 1.6. *Multiplication $(\cdot)$ is well-defined, associative and commutative.*

Proof. First, we show that $\cdot$ is well-defined. Let $a = [(m,n)] = [(m',n')],\ b = [(p,q)] = [(p',q')] \in \mathbb{Z}$. We claim that $a \cdot b = [(mp + nq, mq + np)] = [(m'p' + n'q', m'q' + n'p')]$, i.e. $(mp + nq, mq + np) \sim_{\mathbb{Z}} (m'p' + n'q', m'q' + n'p')$.

From $(p,q) \sim_{\mathbb{Z}} (p',q')$,

$$\begin{aligned} p + q' &= q + p' \\ mp + mq' &= mq + mp' \\ np + nq' &= nq + np' \\ mp + nq + mq' + np' &= mq + np + mp' + nq' \\ (mp + nq, mq + np) &\sim_{\mathbb{Z}} (mp' + nq', mq' + np') \end{aligned}$$

From $(m,n) \sim_{\mathbb{Z}} (m',n')$,

$$\begin{aligned} m + n' &= n + m' \\ mp' + n'p' &= np' + m'p' \\ mq' + n'q' &= nq' + m'q' \\ mp' + nq' + m'q' + n'p' &= mq' + np' + m'p' + n'q' \\ (mp' + nq', mq' + np') &\sim_{\mathbb{Z}} (m'p' + n'q', m'q' + n'p') \end{aligned}$$

Transitivity of $\sim_{\mathbb{Z}}$ yields the desired result.

For $a, b, c \in \mathbb{Z}$, let $a = [(m, n)], b = [(p, q)], c = [(r, s)]$.

$$\begin{aligned}
(a \cdot b) \cdot c &= [(mp + nq, mq + np)] \cdot [(r, s)] \\
&= [((mp + nq)r + (mq + np)s, (mp + nq)s + (mq + np)r)] \\
&= [(mpr + nqr + mqs + nps, mps + nqs + mqr + npr)] \\
a \cdot (b \cdot c) &= [(m, n)] \cdot [(pr + qs, ps + qr)] \\
&= [(m(pr + qs) + n(ps + qr), m(ps + qr) + n(pr + qs))] \\
&= [(mpr + mqs + nps + nqr, mps + mqr + npr + nqs)]
\end{aligned}$$

Therefore, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, i.e. $\cdot$ is associative.

$$\begin{aligned}
a \cdot b &= [(mp + nq, mq + np)] \\
&= [(pm + qn, pn + qm)] \\
&= b \cdot a
\end{aligned}$$

Therefore, $\cdot$ is commutative.

□

Theorem 1.7. *For all $a \in \mathbb{Z}$, $a \cdot \bar{1} = a = \bar{1} \cdot a$.*

Theorem 1.8 (Distributivity). *For all $a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.*

Theorem 1.9 (No zero divisors). *For all $a, b \in \mathbb{Z}$ with $a, b \neq \bar{0}$, we have $a \cdot b \neq \bar{0}$.*

Theorem 1.10 (Cancellation). *For $a, b, c \in \mathbb{Z}$ with $a \neq \bar{0}$, we have $a \cdot b = a \cdot c \Rightarrow b = c$.*

Definition (Order). For all $a, b \in \mathbb{Z}$, we say that $a > b$ if $a - b \in \mathbb{Z}^+$.

Theorem 1.11. *For all $a, b \in \mathbb{Z}$, we have $a \cdot b > 0$ if $a, b > 0$ or $a, b < 0$.*

Definition (Identification map). Define $I_{\mathbb{N}} \colon \mathbb{N} \to \mathbb{Z}$ by

$$I_{\mathbb{N}} := [(n + 1, 1)], \quad \text{for all } n \in \mathbb{Z}.$$

Theorem 1.12. *$I_{\mathbb{N}}$ is injective.*

Theorem 1.13. *$I_{\mathbb{N}}(\mathbb{N}) = \mathbb{Z}^+$.*

Theorem 1.14. *$I_{\mathbb{N}}(1) = \bar{1}$.*

Theorem 1.15. *For all $m, n \in \mathbb{N}$, $I_{\mathbb{N}}(m + n) = I_{\mathbb{N}}(m) + I_{\mathbb{N}}(n)$.*

Theorem 1.16. *For all $m, n \in \mathbb{N}$, $I_{\mathbb{N}}(m \cdot n) = I_{\mathbb{N}}(m) \cdot I_{\mathbb{N}}(n)$.*

Theorem 1.17. *For all $m, n \in \mathbb{Z}$ with $m > n$, $I_{\mathbb{N}}(m) > I_{\mathbb{N}}(n)$.*