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 $\mathbb{N} \times \mathbb{N}$. $\square$

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. $\square$

Lemma 1.3. *For all $m, n, k \in \mathbb{N}$, $[(m, n)] = [(m + k, n + k)] \in \mathbb{Z}$.*

Proof. It is sufficient to show that $(m, n) \sim_{\mathbb{Z}} (m+k, n+k)$, i.e. $m+n+k = n+m+k$, which is certainly true. $\square$

Lemma 1.4. *For all $n \in \mathbb{N}$, $[(n,n)] = \bar{0}$.*

Proof. It is sufficient to show that $(n,n) \sim_{\mathbb{Z}} (1,1)$, i.e. $n+1 = n+1$, which is certainly true. $\square$

Theorem 1.5. *For all $a \in \mathbb{Z}$, $\bar{0} + a = a = a + \bar{0}$.*

Proof. Let $a = [(m,n)] \in \mathbb{Z}$.

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

Theorem 1.6. *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 $a + x' = \bar{0} = x' + a$.

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

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

Corollary 1.6.1. *If $a = [(m,n)] \in \mathbb{Z}$, then $-a = [(n,m)]$.*

Proof. Clearly, $a + (-a) = [(m+n, n+m)] = \bar{0}$. $\square$

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

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

Theorem 1.7. *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 $x = b - a = b + (-a) \in \mathbb{Z}$.

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

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

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

Theorem 1.8. *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 1.9. *For all $a \in \mathbb{Z}$, $a \cdot \bar{1} = a = \bar{1} \cdot a$.*

Proof. Let $a = [(m,n)] \in \mathbb{Z}$.

$$\begin{aligned}
a \cdot \bar{1} &= [(m,n)] \cdot [(2,1)] \\
&= [(2m + n, m + 2n)] \\
&= [(m + (m + n), (m + n) + n)] \\
&= [(m,n)] \\
&= a \\
a \cdot \bar{1} &= a = \bar{1} \cdot a
\end{aligned}$$

□

Theorem 1.10 (Distributivity). *For all $a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.*

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

$$\begin{aligned}
a \cdot (b + c) &= [(m,n)] \cdot [(p + r, q + s)] \\
&= [(m(p + r) + n(q + s), m(q + s) + n(p + r))] \\
&= [(mp + mr + nq + ns, mq + ms + np + nr)] \\
&= [(mp + nq, mq + np)] + [(mr + ns, ms + nr)] \\
&= a \cdot b + a \cdot c
\end{aligned}$$

□

Corollary 1.10.1. *For all $a \in \mathbb{Z}$, $a \cdot \bar{0} = \bar{0}$.*

Proof.

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

□

Corollary 1.10.2. *For all $a, b \in \mathbb{Z}$, $(-a) \cdot b = -(a \cdot b)$.*

Proof.

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

□

Corollary 1.10.3. *For all $a,b\in\mathbb{Z}$, $(-a)\cdot(-b)=a\cdot b$.*

Proof.

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

□

Lemma 1.11. *If $a=[(m,n)]\in\mathbb{Z}$, $a\neq\bar{0}$, then $m\neq n$.*

Proof. Assume that $m=n$. Then, we have $(m,n)\sim_{\mathbb{Z}}\bar{0}$, contradicting our premise. Hence, we must have $m\neq n$. □

Theorem 1.12 (No zero divisors). *For all $a,b\in\mathbb{Z}$ with $a,b\neq\bar{0}$, we have $a\cdot b\neq\bar{0}$.*

Proof. Let $a=[(m,n)], b=[(p,q)]\in\mathbb{Z}$. Note that $m\neq n$, $p\neq n$, since $a,b\neq\bar{0}$.

Assume that our theorem is false, i.e. $a\cdot b=\bar{0}$. Then $(mp+nq,mq+np)\sim_{\mathbb{Z}}\bar{0}\Rightarrow mp+nq=mq+np$. One of the following must be true.

Case I: If $m>n$, there exists $u\in\mathbb{N}$, such that $m=n+u$. Thus, $(n+u)p+nq=(n+u)q+np\Rightarrow np+up+nq=nq+uq+np$. This implies that $up=uq\Rightarrow p=q$, contradicting $p\neq q$.

Case II: If $n>m$, there exists $v\in\mathbb{N}$, such that $n=m+v$. Thus, $mp+(m+v)q=mq+(m+v)p\Rightarrow mp+mq+vq=mq+mp+vp$. This implies that $vp=vq\Rightarrow p=q$, contradicting $p\neq q$.

Hence, $a\cdot b\neq\bar{0}$. □

Theorem 1.13 (Cancellation). *For $a,b,c\in\mathbb{Z}$ with $a\neq\bar{0}$, we have $a\cdot b=a\cdot c\Rightarrow b=c$.*

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

$$\begin{aligned}a\cdot b &= a\cdot c\\ [(mp+nq,mq+np)] &= [(mr+ns,ms+nr)]\\ mp+nq+ms+nr &= mq+np+mr+ns\\ m(p+s)+n(q+r) &= m(q+r)+n(p+s)\end{aligned}$$

Assume that our theorem is false. Thus, $b\neq c$, i.e. $b+(-c)=[(p+s,q+r)]\neq\bar{0}\Rightarrow p+s\neq q+r$. Without loss of generality, let $p+s>q+r$, i.e. $p+s=q+r+x$ for some $x\in\mathbb{N}$.

Thus, $m(q+r+x)+n(q+r)=m(q+r)+n(q+r+x)$. This implies that $mx=nx\Rightarrow m=n$, which contradicts $m\neq n$.

Hence, $b=c$. □

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

Lemma 1.14. *If $m,n\in\mathbb{N}$, $m>n$, i.e. $m=n+x$ for $x\in\mathbb{N}$, then $a=[(m,n)]\in\mathbb{Z}^+$.*

Proof. We must show that $a=[(n+x,n)]\in\mathbb{Z}^+$, i.e. for some $k\in\mathbb{N}$, $(n+x,n)\sim_{\mathbb{Z}}(k+1,1)$, i.e. $n+x+1=n+k+1$. This is clearly true for $k=x$. □

Theorem 1.15. *For all $a,b\in\mathbb{Z}$, we have $a\cdot b>0$ if $a,b>0$ or $a,b<0$.*

Proof. If $a,b>\bar{0}$, then $a,b\in\mathbb{Z}^+$. Thus, $a=[(m+1,1)]$ and $b=[(n+1,1)]$ for some $m,n\in\mathbb{N}$.

$$\begin{aligned}a\cdot b &= [((m+1)(n+1)+(1)(1),(m+1)1+1(n+1))]\\ &= [(mn+m+n+1+1,m+1+n+1)]\\ &= [((m+n+2)+mn,(m+n+2))]\in\mathbb{Z}^+\end{aligned}$$

□

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

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

Theorem 1.16. *$I_{\mathbb{N}}$ is injective.*

Proof. Let $m, n \in \mathbb{N}$

$$\begin{aligned} I_{\mathbb{N}}(m) &= I_{\mathbb{N}}(n) \\ [(m+1,1)] &= [(n+1,1)] \\ (m+1,1) &\sim_{\mathbb{Z}} (n+1,1) \\ m+1+1 &= n+1+1 \\ m &= n \end{aligned}$$

Hence, $I_{\mathbb{N}}$ is injective. □

Theorem 1.17. *$I_{\mathbb{N}}(\mathbb{N}) = \mathbb{Z}^+$.*

Proof. We first show that $I_{\mathbb{N}}(\mathbb{N}) \subseteq \mathbb{Z}^+$. Let $x \in I_{\mathbb{N}}(\mathbb{N})$. Thus, there exists at least one $k \in \mathbb{N}$ such that $x = I_{\mathbb{N}}(k) = [(k+1,1)]$, which implies that $x \in \mathbb{Z}^+$ by definition.

Next, we show that $\mathbb{Z}^+ \subseteq I_{\mathbb{N}}(\mathbb{N})$. Let $x \in \mathbb{Z}^+$. By definition, $x = [(k+1,1)]$ for some $k \in \mathbb{N}$. Clearly, $x = I_{\mathbb{N}}(k) \in I_{\mathbb{N}}(\mathbb{N})$.

Hence, we conclude that $I_{\mathbb{N}}(\mathbb{N}) = \mathbb{Z}^+$. □

Theorem 1.18. *$I_{\mathbb{N}}(1) = \bar{1}$.*

Proof.

$$I_{\mathbb{N}}(1) = [(1+1,1)] = [(2,1)] = \bar{1}$$

□

Theorem 1.19. *For all $m, n \in \mathbb{N}$, $I_{\mathbb{N}}(m+n) = I_{\mathbb{N}}(m) + I_{\mathbb{N}}(n)$.*

Proof.

$$\begin{aligned} I_{\mathbb{N}}(m) + I_{\mathbb{N}}(n) &= [(m+1,1)] + [(n+1,1)] \\ &= [(m+1+n+1, 1+1)] \\ &= [((m+n)+1, 1)] \\ &= I_{\mathbb{N}}(m+n) \end{aligned}$$

□

Theorem 1.20. *For all $m, n \in \mathbb{N}$, $I_{\mathbb{N}}(m \cdot n) = I_{\mathbb{N}}(m) \cdot I_{\mathbb{N}}(n)$.*

Proof.

$$\begin{aligned} I_{\mathbb{N}}(m) \cdot I_{\mathbb{N}}(n) &= [(m+1,1)] \cdot [(n+1,1)] \\ &= [((m+1)(n+1) + (1)(1), (m+1)1 + 1(n+1))] \\ &= [(mn+m+n+1+1, m+n+1+1)] \\ &= [(mn+1,1)] \\ &= I_{\mathbb{N}}(m \cdot n) \end{aligned}$$

□

Theorem 1.21. *For all $m, n \in \mathbb{Z}$ with $m > n$, $I_{\mathbb{N}}(m) > I_{\mathbb{N}}(n)$.*

Proof.

$$\begin{aligned} I_{\mathbb{N}}(m) - I_{\mathbb{N}}(n) &= [(m+1,1)] + (-[(n+1,1)]) \\ &= [(m+1,1)] + [(1,n+1)] \\ &= [(m+1+1, 1+n+1)] \\ &= [(m,n)]. \end{aligned}$$

From 1.14, $[(m,n)] \in \mathbb{Z}^+$. Therefore, $I_{\mathbb{N}}(m) - I_{\mathbb{N}}(n) \in \mathbb{Z}^+ \implies I_{\mathbb{N}}(m) > I_{\mathbb{N}}(n)$, as desired. □