MTH 505: Number Theory **Spring 2017**
Homework 1 **Drew Armstrong**

1.1. From $(\mathbb{N}, \sigma, 0)$ to $(\mathbb{N}, +, \cdot, 0, 1)$. Recall Peano's four axioms for the natural numbers:

(P1) There exists a special element called $0 \in \mathbb{N}$.

(P2) The element 0 is not the successor of any number, i.e.,

$$\forall n \in \mathbb{N}, \sigma(n) \neq 0.$$

(P3) Every number has a unique successor, i.e.,

$$\forall m, n \in \mathbb{N}, (\sigma(m) = \sigma(n)) \Rightarrow (m = n).$$

(P4) *The Induction Principle.* If a set of natural numbers $S \subseteq \mathbb{N}$ contains 0 and is closed under succession, then we must have $S = \mathbb{N}$. In other words, if we have

- $0 \in S$,
- $\forall n \in \mathbb{N}, (n \in S) \Rightarrow (\sigma(n) \in S)$,

then it follows that $S = \mathbb{N}$.

It is strange that these axioms do not tell us how to *add* or *multiply* numbers. In this problem you will investige the steps involved when unpacking Peano's axioms into the structure $(\mathbb{N}, +, \cdot, 0, 1)$.

(a) **Lemma.** If $n \in \mathbb{N}$ and $n \neq 0$, show that there exists a unique $m \in \mathbb{N}$ such that $\sigma(m) = n$. We call this m the *predecessor* of n.

This lemma allows us to define the binary operations $+, \cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ recursively, as follows:

$$a + 0 := a, \tag{1}$$
$$a + \sigma(b) := \sigma(a + b), \tag{2}$$
$$a \cdot 0 := 0, \tag{3}$$
$$a \cdot \sigma(b) := (a \cdot b) + a. \tag{4}$$

Now you will prove that $+$ and $\cdot$ have the desired properties. It is important to prove the following results in the suggested order or you might get stuck. Induction is your **only tool**, so for each problem you should define a certain set of natural numbers $S \subseteq \mathbb{N}$ and then prove that $S = \mathbb{N}$. For example, in part (a) you should fix $a, b \in \mathbb{N}$ and then let $S \subseteq \mathbb{N}$ be the set of $c \in \mathbb{N}$ such that $a + (b + c) = (a + b) + c$.

(b) **Associativity of Addition.** Show that for all $a, b, c \in \mathbb{N}$ we have $a+(b+c) = (a+b)+c$.

(c) **Lemma.** Show that $a + 0 = 0 + a$ and $a + \sigma(0) = \sigma(0) + a$ for all $a \in \mathbb{N}$.

(d) **Commutativity of Addition.** Show that for all $a, b \in \mathbb{N}$ we have $a + b = b + a$.

(e) **Distributive Law.** Show that for all $a, b, c \in \mathbb{N}$ we have $a(b + c) = ab + ac$.

(f) **Associativity of Multiplication.** Show that for all $a, b, c \in \mathbb{N}$ we have $a(bc) = (ab)c$.

(g) **Lemma.** Show that for all $a, b \in \mathbb{N}$ we have $\sigma(a)b = ab + b$. [Hint: Induction on b.]

(h) **Commutativity of Multiplication.** Show that for all $a, b \in \mathbb{N}$ we have $ab = ba$. [Hint: Prove the base case by induction, then use Lemma (g).]

Proof. (a) **Lemma.** The induction step here is trivial; it's the base case that's slightly tricky. Let $S \subseteq \mathbb{N}$ be the set of natural numbers that have a predecessor and let $S' := S \cup \{0\}$. If we can prove that $S' = \mathbb{N}$ then it will follow that every nonzero natural number has a predecessor. First note that $0 \in S'$ by definition. Now assume for induction that $n \in S'$. In this case the number $\sigma(n)$ obviously has the predecessor n and hence $\sigma(n) \in S \subseteq S'$. By (P4) we conclude that $S' = \mathbb{N}$ as desired. Furthermore, if $\sigma(m_1) = n = \sigma(m_2)$ for two numbers m_1, m_2 then it follows from (P3) that $m_1 = m_2$, and we conclude that the predecessor of n is unique.

(b) **Associativity of Addition.** Fix $a, b \in \mathbb{N}$ and let $S \subseteq \mathbb{N}$ be the set of natural numbers $c \in \mathbb{N}$ such that $a + (b + c) = (a + b) + c$. We want to prove that $S = \mathbb{N}$. First note that $0 \in S$ because

$$\begin{aligned} a + (b + 0) &= a + b && (1) \\ &= (a + b) + 0. && (1) \end{aligned}$$

Now suppose that $n \in S$ so that $a + (b + n) = (a + b) + n$. In this case we must also have

$$\begin{aligned} a + (b + \sigma(n)) &= a + \sigma(b + n) && (2) \\ &= \sigma(a + (b + n)) && (2) \\ &= \sigma((a + b) + n) && n \in S \\ &= (a + b) + \sigma(n), && (2) \end{aligned}$$

which means that $\sigma(n) \in S$. We conclude from (P4) that $S = \mathbb{N}$ as desired.

(c) **Lemma.** Let $S \subseteq \mathbb{N}$ be the set of natural numbers $a \in \mathbb{N}$ such that $a + 0 = 0 + a$ and let $T \subseteq \mathbb{N}$ be the set of natural numbers $a \in \mathbb{N}$ such that $a + \sigma(0) = \sigma(0) + a$. We will show that $S = T = \mathbb{N}$. First note that $0 \in S$ because equation (1) says that $0 + 0 = 0$. Now suppose that $n \in S$ so that $0 + n = n + 0$. In this case we also have

$$\begin{aligned} 0 + \sigma(n) &= \sigma(0 + n) && (2) \\ &= \sigma(n + 0) && n \in S \\ &= \sigma(n) && (1) \\ &= \sigma(n) + 0, && (1) \end{aligned}$$

and hence $\sigma(n) \in S$. We conclude from (P4) that $S = \mathbb{N}$ as desired.

To show that $T = \mathbb{N}$ we first use the fact that $\sigma(0) \in \mathbb{N} = S$ tells us that (i.e., $\sigma(0)+0 = 0+\sigma(0)$) which tells us that $0 \in T$. Now suppose that $n \in T$ so that $n + \sigma(0) = \sigma(0) + n$. In this case we must also have

$$\begin{aligned} \sigma(0) + \sigma(n) &= \sigma(0) + \sigma(n + 0) && (1) \\ &= \sigma(0) + (n + \sigma(0)) && (2) \\ &= (\sigma(0) + n) + \sigma(0) && (b) \\ &= (n + \sigma(0)) + \sigma(0) && n \in S \\ &= \sigma(n + 0) + \sigma(0) && (2) \\ &= \sigma(n) + \sigma(0), && (1) \end{aligned}$$

and hence $\sigma(n) \in T$. From (P4) it follows that $T = \mathbb{N}$ as desired.

(d) **Commutativity of Addition.** Fix $a \in \mathbb{N}$ and let $S \subseteq \mathbb{N}$ be the set of natural numbers $b \in \mathbb{N}$ such that $a + b = b + a$. We will show that $S = \mathbb{N}$. First recall from part (c) that $0 \in S$.

Now suppose that $n \in S$ so that $a + n = n + a$. In this case we also have

$$\begin{aligned} a + \sigma(n) &= \sigma(a + n) && (2) \\ &= \sigma(n + a) && n \in S \\ &= n + \sigma(a) && (2) \\ &= n + \sigma(a + 0) && (1) \\ &= n + (a + \sigma(0)) && (2) \\ &= n + (\sigma(0) + a) && (c) \\ &= (n + \sigma(0)) + a && (b) \\ &= \sigma(n + 0) + a && (2) \\ &= \sigma(n) + a, && (1) \end{aligned}$$

and hence $\sigma(n) \in S$. From (P4) we conclude that $S = \mathbb{N}$ as desired.

(e) **Distributive Law.** Fix $a, b \in \mathbb{N}$ and let $S \subseteq \mathbb{N}$ be the set of $c \in \mathbb{N}$ such that $a(b + c) = ab + ac$. We will show that $S = \mathbb{N}$. First note that $0 \in S$ because

$$\begin{aligned} a(b + 0) &= ab && (1) \\ &= ab + 0 && (1) \\ &= ab + a0. && (3) \end{aligned}$$

Now assume that $n \in S$ so that $a(b + n) = ab + an$. In this case we must also have

$$\begin{aligned} a(b + \sigma(n)) &= a\sigma(b + n) && (2) \\ &= a(b + n) + a && (4) \\ &= (ab + an) + a && n \in S \\ &= ab + (an + a) && (b) \\ &= ab + a\sigma(n), && (4) \end{aligned}$$

and hence $\sigma(n) \in S$. From (P4) we conclude that $S = \mathbb{N}$ as desired.

(f) **Associativity of Multiplication.** Fix $a, b \in \mathbb{N}$ and let $S \subseteq \mathbb{N}$ be the set of $c \in \mathbb{N}$ such that $a(bc) = (ab)c$. We will show that $S = \mathbb{N}$. First note that $0 \in S$ because

$$\begin{aligned} a(b0) &= a0 && (3) \\ &= 0 && (3) \\ &= (ab)0. && (3) \end{aligned}$$

Now assume that $n \in S$ so that $a(bn) = (ab)n$. In this case we must also have

$$\begin{aligned} a(b\sigma(n)) &= a(bn + b) && (4) \\ &= a(bn) + ab && (e) \\ &= (ab)n + ab && n \in S \\ &= (ab)\sigma(n), && (4) \end{aligned}$$

and hence $\sigma(n) \in S$. From (P4) we conclude that $S = \mathbb{N}$ as desired.

(g) **Lemma.** Fix $a \in \mathbb{N}$ and let $S \subseteq \mathbb{N}$ be the set of $b \in \mathbb{N}$ such that $\sigma(a)b = ab + b$. We will show that $S = \mathbb{N}$. First note that $0 \in S$ because

$$\begin{aligned} \sigma(a)0 &= 0 && (3) \\ &= a0 && (3) \\ &= a0 + 0. && (1) \end{aligned}$$

Now suppose that $n \in S$ so that $\sigma(a)n = an + n$. In this case we must also have

$$\begin{aligned}
\sigma(a)\sigma(n) &= \sigma(a)n + \sigma(a) && (4)\\
&= (an + n) + \sigma(a) && n \in S\\
&= an + (n + \sigma(a)) && (b)\\
&= an + \sigma(n + a) && (2)\\
&= an + \sigma(a + n) && (d)\\
&= an + (a + \sigma(n)) && (2)\\
&= (an + a) + \sigma(n) && (b)\\
&= a\sigma(n) + \sigma(n), && (4)
\end{aligned}$$

and hence $\sigma(n) \in S$. From (P4) we conclude that $S = \mathbb{N}$ as desired.

(h) **Commutativity of Multiplication.** Finally, fix $a \in \mathbb{N}$ and let $S \subseteq \mathbb{N}$ be the set of $b \in \mathbb{N}$ such that $ab = ba$. We will show that $S = \mathbb{N}$. First we will show that $0 \in S$. To do this, let $T \subseteq \mathbb{N}$ be the set of $a \in \mathbb{N}$ such that $a0 = 0a$. Note that $0 \in T$ by property (3) and assume that $n \in T$ so that $n0 = 0n$. It then follows that

$$\begin{aligned}
0\sigma(n) &= 0n + 0 && (4)\\
&= 0n && (1)\\
&= n0 && n \in T\\
&= 0 && (3)\\
&= \sigma(n)0, && (3)
\end{aligned}$$

and hence $\sigma(n) \in T$. By (P4) we conclude that $T = \mathbb{N}$ and hence $0 \in S$. Now suppose that $n \in S$ so that $an = na$. In this case we must also have

$$\begin{aligned}
a\sigma(n) &= an + a && (4)\\
&= na + a && n \in S\\
&= \sigma(n)a, && (f)
\end{aligned}$$

and hence $\sigma(n) \in S$. From (P4) we conclude that $S = \mathbb{N}$ as desired. □

[Remark: That was kind of tricky right? And we didn't even try to investigate the properties of the total ordering $(\mathbb{N}, \leqslant)$.]

1.2. From $(\mathbb{N}, +, \cdot, 0, 1)$ to $(\mathbb{Z}, +, \cdot, 0, 1)$. The integers are obtained from the natural numbers by "formally adjoining additive inverses". This problem will investigate the steps involved. Let $(\mathbb{N}, +, \cdot, 0, 1)$ be the structure obtained from Problem 1.1. You can ignore the successor function now and just write $n + 1$ instead of $\sigma(n)$. Let $\mathbb{Z}$ denote the set of ordered pairs of natural numbers:

$$\mathbb{Z} = \{[a, b] : a, b \in \mathbb{N}\}.$$

(a) Prove that the following rule defines an equivalence relation on $\mathbb{Z}$:

$$[a, b] \sim [c, d] \quad \Longleftrightarrow \quad a + d = b + c.$$

Intuition: We think of the pair $[a, b]$ as the fictional number "$a - b$".

(b) Prove that the following binary operations on $\mathbb{Z}$ are well-defined on equivalence classes:

$$\begin{aligned}
[a, b] + [c, d] &:= [a + c, b + d],\\
[a, b] \cdot [c, d] &:= [ac + bd, ad + bc].
\end{aligned}$$

(c) Prove that each of the operations $+, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is commutative and associative, and also that $\cdot$ distributes over $+$.

(d) Finally, explain how to view $(\mathbb{N}, +, \cdot, 0, 1)$ as subsystem of $(\mathbb{Z}, +, \cdot, 0, 1)$ and show that each element of $\mathbb{N}$ now has an *additive inverse* in the larger system.

Apology: I should have said that you are allowed to use multiplicative and additive cancellation in $\mathbb{N}$ without proving them. Sorry.

Proof. (a) To show that $\sim$ is reflexive, note that $a + b = a + b$ implies $[a, b] \sim [a, b]$ for all $[a, b] \in \mathbb{Z}$. To show that $\sim$ is symmetric, assume that we have $[a, b] \sim [c, d]$, i.e., that $a + d = b + c$. Then by commutativity of addition in $\mathbb{N}$ we also have $c + b = d + a$ which says that $[c, d] \sim [a, b]$ as desired. Finally, to show that $\sim$ is transitive, assume that $[a, b] \sim [c, d]$ and $[c, d] \sim [e, f]$, i.e. that $a + d = b + c$ and $c + f = d + e$. In this case we have

$$\begin{aligned}(a + f) + d &= (a + d) + f \\ &= (b + c) + f \\ &= (c + f) + b \\ &= (d + e) + b \\ &= (b + e) + d.\end{aligned}$$

Then from additive cancellation we conclude that $a + f = e + b$, i.e., that $[a, b] \sim [e, f]$.

(b) Assume that we have $[a, b] \sim [a', b']$ (i.e., $a + b' = a' + b$) and $[c, d] \sim [c', d']$ (i.e., $c + d' = c' + d$). In this case we want to show that

$$\begin{aligned}[a, b] + [c, d] &\sim [a', b'] + [c', d'], \\ [a, b] \cdot [c, d] &\sim [a', b'] \cdot [c', d'].\end{aligned}$$

To show the first equation recall that $[a, b] + [c, d] = [a + c, b + d]$ and $[a', b'] + [c', d'] = [a' + c', b' + d']$. Then observe that we have

$$\begin{aligned}(a + c) + (b' + d') &= (a + b') + (c + d') \\ &= (a' + b) + (c' + d) \\ &= (a' + c') + (b + d),\end{aligned}$$

which tells us that $[a + c, b + d] \sim [a' + c', b' + d']$ as desired. Next recall that $[a, b] \cdot [c, d] = [ac + bd, ad + bc]$ and $[a', b'] \cdot [c', d'] = [a'c' + b'd', a'd' + b'c']$. Our goal is to show that $[ac + bd, ad + bc] \sim [a'c' + b'd', a'd' + b'c']$ or in other words that

$$(ac + bd) + (a'd' + b'c') = (a'c' + b'd') + (ad + bc). \qquad (*)$$

To show this we first use the facts $a + b' = a' + b$ and $c + d' = c' + d$ to observe that

$$c(a + b') + d(a' + b) + a'(c + d') + b'(c' + d) = d(a + b') + c(a' + b) + b'(c + d') + a'(c' + d)$$

Then we expand and rearrange each side to obtain

$$(ac + bd + a'd' + b'c') + (b'c + a'd + a'c + b'd) = (a'c' + b'd' + ad + bc) + (b'c + a'd + a'c + b'd).$$

Finally, we cancel $(b'c + a'd + a'c + b'd)$ from both sides to obtain $(*)$ as desired.

(c) I'm going to treat this problem as optional for myself.

(d) To view $(\mathbb{N}, +, \cdot, 0, 1)$ as a subsystem of $(\mathbb{Z}, +, \cdot, 0, 1)$ we identify each natural number $n \in \mathbb{N}$ with (the eqivalence class of) the integer $[n, 0]$. Note that this identification is one-to-one because we have $[m, 0] \sim [n, 0]$ if and only if $m = n$. Finally, note that the identification preserves the operations $+$ and $\cdot$ because

$$[m, 0] + [n, 0] = [m + n, 0],$$
$$[m, 0] \cdot [n, 0] = [mn, 0].$$

□

Apology: For the next problem I will freely use all of the friendly properties of $\mathbb{Z}$ without proving them from the Peano axioms.

1.3. From $(\mathbb{Z}, +, \cdot, 0, 1)$ to $(\mathbb{Q}, +, \cdot, 0, 1)$. The rational numbers are obtained from the natural numbers by "formally adjoining multiplicative inverses". This problem will investigate the steps involved. Let $(\mathbb{Z}, +, \cdot, 0, 1)$ be the structure obtained from Problem 1.2. But now we will forget the language of ordered pairs and we will just write $n \in \mathbb{Z}$ for integers. Let $\mathbb{Q}$ denote the set of **ordered pairs of integers** in which the second entry is **nonzero**:

$$\mathbb{Q} := \{[a, b] : a, b \in \mathbb{Z}, b \neq 0\}.$$

(a) Prove that the following rule defines an equivalence relation on $\mathbb{Q}$:

$$[a, b] \sim [c, d] \quad \Longleftrightarrow \quad ad = bc.$$

Intuition: We think of the pair $[a, b]$ as the fictional number "a/b".

(b) Prove that the following binary operations on $\mathbb{Q}$ are well-defined on equivalence classes:

$$[a, b] \cdot [c, d] := [ac, bd],$$
$$[a, b] + [c, d] := [ad + bc, bd].$$

Hence we obtain two binary operations $+, \cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$.

(c) **(Optional)** Prove that each of the operations $+, \cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ is commutative and associative, and also that $\cdot$ distributes over $+$.

(d) Finally, explain how to view $(\mathbb{Z}, +, \cdot, 0, 1)$ as subsystem of $(\mathbb{Q}, +, \cdot, 0, 1)$ and show that each **nonzero** element of $\mathbb{Z}$ now has an *multiplicative inverse* in the larger system.

Proof. (a) To show that $\sim$ is reflexive, note that the commutative rule $ab = ba$ implies that $[a, b] \sim [a, b]$ for all $[a, b] \in \mathbb{Q}$. To show that $\sim$ is symmetric assume that we have $[a, b] \sim [c, d]$, i.e., that $ad = bc$. Then by commutativity we must have $cb = da$ and hence $[c, d] \sim [a, b]$. Finally, to show that $\sim$ is transitive, assume that $[a, b] \sim [c, d]$ and $[c, d] \sim [e, f]$, i.e., that $ad = bc$ and $cf = de$. Recall that we also have $d \neq 0$ by definition of $\mathbb{Q}$. Now there are two cases. If $c = 0$ then the fact $ad = bc = 0$ together with $d \neq 0$ implies $a = 0$ and the fact $cf = de = 0$ together with $d \neq 0$ implies $e = 0$. Then putting these together gives

$$af = 0 = be$$

and hence $[a, b] \sim [e, f]$ as desired. On ther other hand, if $c \neq 0$ then since $d \neq 0$ we also have $cd \neq 0$. Then multiplying the equations $ad = bc$ and $cf = de$ gives

$$(ad)(cf) = (bc)(de)$$
$$(af)(cd) = (be)(cd),$$

and cancelling the nonzero factor cd gives $af = be$, and hence $[a, b] \sim [e, f]$ as desired.

(b) Assume that we have $[a,b] \sim [a',b']$ (i.e., $ab' = a'b$) and $[c,d] \sim [c',d']$ (i.e., $cd' = c'd$). In this case we want to show that

$$[a,b] \cdot [c,d] \sim [a',b'] \cdot [c',d'],$$
$$[a,b] + [c,d] \sim [a',b'] + [c',d'].$$

To show the first equation recall that $[a,b] \cdot [c,d] = [ac,bd]$ and $[a',b'] \cdot [c',d'] = [a'c',b'd']$. Now multiply the equations $ab' = a'b$ and $cd' = c'd$ to obtain

$$(ab')(cd') = (a'b)(c'd)$$
$$(ac)(b'd') = (a'c')(bd),$$

which tells us that $[ac,bd] \sim [a'c',b'd']$ as desired. Next recall that $[a,b]+[c,d] = [ad+bc,bd]$ and $[a',b'] + [c',d'] = [a'd' + b'c', b'd']$. Then we have

$$\begin{aligned}(ad+bd)(b'd') &= (ad)(b'd') + (bc)(b'd') \\ &= (ab')(dd') + (cd')(bb') \\ &= (a'b)(dd') + (c'd)(bb') \\ &= (a'd')(bd) + (b'c')(bd) \\ &= (a'd' + b'c')(bd),\end{aligned}$$

which tells us that $[a,b] + [c,d] \sim [a',b'] + [c',d']$ as desired.

(c) This was optional for everyone (including me).

(d) To view $(\mathbb{Z}, +, \cdot, 0, 1)$ as a subsystem of $(\mathbb{Q}, +, \cdot, 0, 1)$ we identify each integer $n \in \mathbb{Z}$ with (the equivalence class of) the rational number $[n,1]$. Note that this identification is one-to-one because we have $[m,1] \sim [n,1]$ if and only if $m = n$. Note that this identification preserves the operations $+$ and $\cdot$ because

$$[m,1] + [n,1] = [m+n,1],$$
$$[m,1] \cdot [n,1] = [mn,1].$$

Finally, observe that each nonzero rational number has a multiplicative inverse. Indeed, given any $[a,b] \nsim [0,1]$ we must have $a \neq 0$ and hence the rational number $[b,a]$ is defined. Then observe that

$$[a,b] \cdot [b,a] = [1,1]$$

as desired. □

[Remark: This HW was a sketch of how the entire apparatus of number systems can be built from the Peano axioms. This apparatus is called Peano Arithmetic (PA). Filling in all of the details would take a very long time and some might feel that we already spent too long on this.

Most mathematicians believe that PA is "consistent", i.e., that it will never lead to a contradiction. A student asked me after class whether the consistency of PA can be proved. Gödel (1931) showed that **the consistency of PA can not be proved within PA**. Gentzen (1936) showed that the consistency of PA **can be proved** by passing to a much more complicated and less intuitive system such as the Zermelo-Fraenkel axioms for set theory. Gödel's result still leaves open the possibility that **PA is inconsistent**, and occasionally a mathematician or a crank will claim to have proved this. As far as I know all of the proofs have been wrong. It does not surprise me that human intuition is difficult to formalize.]