ELEMENTARY NUMBER THEORY

HOMEWORK 1

(1) Prove the cancellation law in $\mathbb{N}$: if $x, y, z \in \mathbb{N}$ satisfy $x + z = y + z$, then $x = y$.

Statements about natural numbers have to be proved by induction (what else?). Thus take $x, y \in \mathbb{N}$ and set $S = \{z \in \mathbb{N} : x + z = y + z \Longrightarrow x = y\}$. Then clearly $0 \in S$ since $x + 0 = x$ and $y + 0 = y$. Now assume that $z \in S$; we have to show $s(z) \in S$. Suppose therefore that $x + s(z) = y + s(z)$. Since $x + s(z) = s(x + z)$ we see that $s(x + z) = s(y + z)$. By Axiom N4 we conclude that $x + z = y + z$, and the induction assumption gives $x = y$. Thus $s(x) \in S$, hence $S = \mathbb{N}$.

The following proof is not correct as it stands: Suppose therefore that $x+s(z) = y+s(z)$. We have proved that $x+s(z) = s(x)+z$ and $y+s(z) = s(y) + z$; this shows $s(x) + z = s(y) + z$. By induction assumption, this implies $s(x) = s(y)$, hence $x = y$.

Where is the error? The induction assumption tells us what to do with $x + z = y + z$, not with $s(x) + z = s(y) + z$ (look at the definition of the set S if you don't believe me)!

(2) Consider the set $N = \{0, 1\}$ with successor function $s : N \longrightarrow N$ mapping $0 \longmapsto 1$ and $1 \longmapsto 0$. Show that this system satisfies all Peano axioms except one – which one?

- N1: $0 \in N$
- N2: $x \in N$ implies $s(x) \in N$
- N3: not satisfied since $s(1) = 0$
- N4: s is injective
- N5: if S contains 0 and $s(0)$, then $S = N$.

Thus only N3 is not satisfied.

(3) Show that $[r, s] * [t, u] = [rt, su]$ is not well defined on $\mathbb{Z}$.

We have $[2, 1] * [2, 1] = [4, 1]$; but $[2, 1] = [3, 2]$ and $[3, 2] * [3, 2] = [9, 4]$ although $[4, 1] \neq [9, 4]$.

(4) Prove that addition on $\mathbb{Z}$ is commutative.

This is done by reduction to $\mathbb{N}$:

$$\begin{aligned} [r, s] + [t, u] &= [r + t, s + u] && \text{by definition of addition} \\ &= [t + r, u + s] && \text{by commutativity in } \mathbb{N} \\ &= [t, u] + [r, s] && \text{by definition of addition} \end{aligned}$$

(5) Consider the monoid $M = 2\mathbb{Z} \cup \{1\} = \{1, 2, 4, 6, 8, \ldots\}$. Show that M does not contain any prime, and find all irreducible elements in M.

bigskip

1 is not a prime because it is a unit. Every nonunit has the form $2n$ for some $n \in \mathbb{N}$. Then $2n \mid 6n \cdot (6n)$ because $6n \cdot 6n = 36n^2$ and $36n^2 = 2n \cdot 18n$. On the other hand, $2n \nmid 6n$ because the quotient 3 is not in M. Thus M has no primes.

What are the irreducible elements? We can factor $4n = 2 \cdot 2n$, so elements o the form $4n$ are not irreducible. We claim that $4n + 2$ is irreducible. If not, then it has to have a nontrivial factorization (one not involving the unit 1), hence $4n + 2 = (2r)(2s)$; but this is nonsense since the right hand side is divisible by 4. Thus the irreducible elements are those of the form $4n + 2$.