MSGSÜ, MAT 221, Sınav, 10 Kasım 2014, Saat 13:00, David Pierce. *Sadece 4 soruyu cevaplayın.*

As in class, $\mathbb{N}$ is the set $\{1, 2, 3, \ldots\}$ of **natural numbers,** and $x'$ is the **successor** of $x$, so $1' = 2$, $2' = 3$, and so on. We also let $\omega = \{0\} \cup \mathbb{N}$ and $0' = 1$.

**Problem 1.** For a given value of $n$ in $\mathbb{N}$, let $\bar{x}$ denote the congruence-class of $x$ *modulo* $n$, and let $\mathbb{Z}_n = \{\bar{x} \colon x \in \mathbb{N}\} = \{\bar{1}, \ldots, \bar{n}\}$. If $\overline{x'} = \overline{y'}$, then $\bar{x} = \bar{y}$. Therefore we can define $\bar{x}\,' = \overline{x'}$. The structure $(\mathbb{Z}_n, \bar{1}, ')$ allows proofs by induction. We have shown that addition and multiplication on $\mathbb{Z}_n$ can be defined recursively by

$$\begin{aligned} \bar{x} + \bar{1} &= \bar{x}\,', & \bar{x} + \bar{y}\,' &= (\bar{x} + \bar{y})\,', \\ \bar{x} \cdot \bar{1} &= \bar{x}, & \bar{x} \cdot \bar{y}\,' &= \bar{x} \cdot \bar{y} + \bar{x}. \end{aligned}$$

(a) If $n = 6$, show that there is an operation on $\mathbb{Z}_n$ given by

$$\bar{x}^{\bar{1}} = \bar{x}, \qquad \bar{x}^{\bar{y}'} = \bar{x}^{\bar{y}} \cdot \bar{x}. \qquad (*)$$

It is enough to fill out the table [in the solution].

(b) If $n = 3$, show that there is *no* operation on $\mathbb{Z}_n$ as in $(*)$.

*Solution.*

(a)

| $\bar{x}^{\bar{y}}$ | | $y$ | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 |
| $x$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 2 | 2 | 4 | 2 | 4 | 2 | 4 |
| | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| | 5 | 5 | 2 | 5 | 2 | 5 | 2 |
| | 6 | 6 | 6 | 6 | 6 | 6 | 6 |

From the table it should be clear that, *modulo* 6,

$$a \equiv b \implies x^a \equiv x^b.$$

(b) Using $(*)$, we obtain $\bar{2}^{\bar{1}} = \bar{2}$, $\bar{2}^{\bar{2}} = \bar{4} = \bar{1}$, $\bar{2}^{\bar{3}} = \bar{2}$, so $\bar{2}^{\bar{4}} = \bar{1}$, so $\bar{2}^{\bar{1}} \neq \bar{2}^{\bar{4}}$, although $\bar{1} = \bar{4}$.

**Problem 2.** Using only the recursive definition of addition on $\mathbb{N}$ and induction, prove that addition is associative.

*Solution.* We want to show $x + (y + z) = (x + y) + z$.

1. By the recursive definition of addition (namely $x+1 = x'$ and $x + y' = (x + y)')$, we have

$$x + (y + 1) = x + y' = (x + y)' = (x + y) + 1,$$

so the claim is true when $z = 1$.

2. Suppose the claim is true when $z = t$. Then

$$\begin{aligned} x + (y + t') &= x + (y + t)' && \text{[def'n of +]} \\ &= (x + (y + t))' && \text{[def'n of +]} \\ &= ((x + y) + t)' && \text{[inductive hypothesis]} \\ &= (x + y) + t', && \text{[def'n of +]} \end{aligned}$$

so the claim is true when $z = t'$.

By induction, the claim holds for all $z$ in $\mathbb{N}$ (for all $x$ and $y$ in $\mathbb{N}$).

**Problem 3.** We know $2 \cdot \sum_{k=1}^{n} k = n \cdot (n + 1)$. For all $n$ in $\mathbb{N}$, prove

$$\left( \sum_{k=1}^{n} k \right)^2 = \sum_{k=1}^{n} k^3.$$

*Solution.* The claim is obvious when $n = 1$. Suppose it is true when $n = m$. Then

$$\left( \sum_{k=1}^{m+1} k \right)^2 = \left( \sum_{k=1}^{m} k \right)^2 + 2 \cdot \sum_{k=1}^{m} k \cdot (n + 1) + (n + 1)^2$$

$$= \sum_{k=1}^{n} k^3 + n \cdot (n + 1)^2 + (n + 1)^2 = \sum_{k=1}^{n} k^3 + (n + 1)^3 = \sum_{k=1}^{n+1} k^3.$$

**Problem 4.** We can define the so-called binomial coefficients recursively by

$$\binom{0}{0} = 1, \qquad \binom{0}{k+1} = 0,$$
$$\binom{n+1}{0} = 1, \qquad \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$$

Using only this definition, and induction, show that, for all $n$ in $\omega$,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

*Solution.* The claim is obvious when $n = 0$. Suppose it is true when $n = m$. Then

$$\begin{aligned}
\sum_{k=0}^{m+1} \binom{m+1}{k} = \binom{m+1}{0} + \sum_{k=0}^{m} \binom{m+1}{k+1} \\
&= 1 + \sum_{k=0}^{m} \left( \binom{m}{k} + \binom{m}{k+1} \right) \\
&= \sum_{k=0}^{m} \binom{m}{k} + \sum_{k=0}^{m+1} \binom{m}{k} \\
&= \sum_{k=0}^{m} \binom{m}{k} + \sum_{k=0}^{m} \binom{m}{k} = 2 \cdot 2^m = 2^{m+1}
\end{aligned}$$

(since $\binom{m+1}{0} = 1 = \binom{m}{0}$ and $\binom{m}{m+1} = 0$). Therefore, by induction, the claim is true for all $n$ in $\omega$. (We do not have $\binom{m}{m+1} = 0$ immediately from the definition, but can prove by induction that $\binom{m}{n} = 0$ when $n > m$.)

**Problem 5.** Let $d$ be the greatest common divisor of 385 and 168.

(a) Find $d$.

(b) Find a solution from $\mathbb{N}$ of one of the equations

$$385x = 168y + d, \qquad\qquad 168x = 365y + d.$$

*Solution.*

(a) Since

$$\begin{aligned} 385 &= 168 \cdot 2 + 49 \\ 168 &= 49 \cdot 3 + 21 \\ 49 &= 21 \cdot 2 + 7 \end{aligned}$$

and $7 \mid 21$, we conclude $\gcd(385, 168) = 7$.

(b) From the previous computations,

$$\begin{aligned} 7 &= 49 - 21 \cdot 2 \\ &= 49 - (168 - 49 \cdot 3) \cdot 2 \\ &= 49 \cdot 7 - 168 \cdot 2 \\ &= (385 - 168 \cdot 2) \cdot 7 - 168 \cdot 2 \\ &= 385 \cdot 7 - 168 \cdot 16. \end{aligned}$$

Thus $385 \cdot 7 = 168 \cdot 16 + 7$.