An answer to Exercise 5.9

Let I be a nonempty subset of the natural numbers $\mathbb{N} = \{1, 2, 3, \cdots\}$.

The set S is defined to be least subset of $\mathbb{N}$ such that

$I \subseteq S$, and
if $m, n \in S$ and $m < n$, then $(n - m) \in S$.

Define h to be the least member of S. This question guides you through to a proof that h coincides with the *highest common factor* of I, written $hcf(I)$, and defined to be the natural number with the properties that

$hcf(I)$ divides n for every element $n \in I$, and
if k is a natural number which divides n for every $n \in I$, then k divides $hcf(I)$.

(a) The set S may also be described as the least subset of $\mathbb{N}$ closed under certain rules.

Describe the rules.

$$\frac{}{i}\quad i \textit{ in } I \qquad\qquad \frac{n\ ,\quad m}{n-m}\quad m < n \textit{ in } \mathbb{N}$$

Write down a principle of rule induction appropriate for the set S.

A property $P(x)$ holds for all $x \in S$ iff
$\forall i \textit{ in } I.\, P(i)$ *and*
$\forall m < n \textit{ in } \mathbb{N}.\, P(n) \,\&\, P(m) \Rightarrow P(n - m)$

(b) Show by rule induction that $hcf(I)$ divides n for every $n \in S$.

Consider the property $P(x)$ given by $hcf(I)$ divides x.

Base case: We need show that $hcf(I)$ divides i for all i in I; which holds by definition of $hcf(I)$.

Inductive step: Let $m < n$ in $\mathbb{N}$ be such that $hcf(I)$ divides n and m. We need show that $hcf(I)$ divides $n - m$.
By assumption, $n = l \cdot hcf(I)$ for some $l \in \mathbb{N}$ and $m = k \cdot hcf(I)$ for some $k \in \mathbb{N}$. Hence, $n - m = (l - k) \cdot hcf(I)$ for $(l - k) \in \mathbb{N}$, as $n > m$, and we are done.

(c) Let $n \in S$. Establish that

$$\text{if } \ p \cdot h < n \ \text{ then } \ (n - p \cdot h) \in S$$

for all nonnegative integers p.

The idea is that since n and h are in S then so will be $n - h$ whenever $n > h$, in which case so will be $(n - h) - h = n - 2 \cdot h$ whenever $n > 2 \cdot h$, etc. Formalise this as an inductive argument on $p \in \mathbb{N}_0$.

(d) Show that h divides n for every $n \in S$. [Hint: suppose otherwise and derive a contradiction.]

> *Suppose that there is an $n \in S$ such that h does not divide it. Since $h < n$, $n = p \cdot h + r$ for $p \in \mathbb{N}_0$ and $0 < r < h$. Then, by the previous item, $r = n - p \cdot h$ is an element of S that happens to be smaller than h. A contradiction!*

(e) Why do the results of (b) and (d) imply that $h = hcf(I)$?

> *Please finish it off.*