Computability Assignment
Year 2012/13 - Number 5

Please keep this file anonymous: do not write your name inside this file.

More information about assignments at http://disi.unitn.it/~zunino/teaching/computability/assignments

Please do not submit a file containing only the answers; edit this file, instead, filling the answer sections.

1 Question

Prove by induction that $\forall k \in \mathbb{N}.\ 9^k - 2^k$ is a multiple of 7. Follow the steps outlined below.

1. Prove that, if $k = 0$, then $9^0 - 2^0$ is a multiple of 7. This is the basis of the induction.

2. Now, suppose that for a *generic* natural number n, it is true that $9^n - 2^n$ is a multiple of 7. By only using this *inductive hypothesis*, prove that $9^{n+1} - 2^{n+1}$ is a multiple of 7. To do so, use the identity:

$$9^{n+1} - 2^{n+1} = 9^{n+1} - 9^n \cdot 2 + 9^n \cdot 2 - 2^{n+1}$$

   and a clever factorization of the right-hand side of the equality. Remember that, at some point, you are expected to use the *inductive hypothesis*.

1.1 Answer

1. $9^0 - 2^0 = 1 - 1 = 0$ which is of course a multiple of 7, in fact $7 \cdot 0 = 0$.

2. $9^{n+1} - 2^{n+1} = 9^{n+1} - 9^n \cdot 2 + 9^n \cdot 2 - 2^{n+1} = 9^n \cdot (9 - 2) + 2 \cdot (9^n - 2^n) = 9^n \cdot 7 + 2 \cdot (9^n - 2^n)$. The first addend is obviously a multiple of seven. By the inductive hypothesis, the second is a multiple of seven too. It means that $\exists n \in \mathbb{N}.(9^n - 2^n) = 7 \cdot n$. Then we have $9^{n+1} - 2^{n+1} = 9^n \cdot 7 + 2 \cdot 7 \cdot n = 7 \cdot (9^n + 2 \cdot n)$. We have finally that $9^{n+1} - 2^{n+1}$ is a multiple of seven.

2 Preliminaries

Let $P(k)$ be the property "$\forall n, m \in \mathbb{N}.\ max(n, m) = k$ implies $n = m$". The following is a proof by induction that $\forall k \in \mathbb{N}.P(k)$.

1. Basis of the induction: if $max(n, m) = 0$ then $n = m = 0$, as we wanted.

2. Inductive step: suppose that $P(k)$ is true for a generic natural number k; we want to prove that this implies $P(k + 1)$, i.e. that for all natural numbers n, m such that $max(n, m) = k + 1$, $n = m$. So, let $n, m \in \mathbb{N}$ satisfy $max(n, m) = k+1$. Then $max(n-1, m-1) = max(n, m)-1 = k$. By the induction hypothesis, it follows that $n - 1 = m - 1$, and therefore $n = m$. This proves $P(k + 1)$, so the induction step is complete.

3 Question

Is the above proof correct? If not, can you tell what is wrong with it?

3.1 Answer

No, it isn't. For example, we have $max(4, 5) = 5$ which of course doesn't imply that $4 = 5$. We take two generic elements $n, m \in \mathbb{N}$, which means that also zero is allowed. The problem rise when we take $n - 1, m - 1$, which aren't in $\mathbb{N}$ if one or both are equal to zero. This could suggest to proove $P(k)$ in $\mathbb{Z}$ but, of course, it's wrong also there: in $\mathbb{Z}$ it isn't even possible to proove the basis of the induction!