Model Solution Homework 10

Saskia van den Hoeven

1. Let $n, m \in \mathbb{Z}_+$. Prove that $n|m$ if and only if $p^n - 1|p^m - 1$.
Solution: Suppose $n|m$. Then

$$p^m - 1 = (p^n - 1)(1 + p^n + \ldots + p^{(k-1)n})$$

for $m = nk$ so $p^n - 1|p^m - 1$. (1 point)
Now suppose $p^n - 1|p^m - 1$. Let $m = qn + r$ with $0 \leq r < n$. Then

$$p^{qn+r} - 1 = (p^n - 1) \cdot (p^{(q-1)n+r} + \ldots + p^{n+r} + p^r) + p^r - 1$$

and $p^n - 1|p^m - 1$ so $p^n - 1|p^r - 1$. But also $p^r - 1 < p^n - 1$, so $p^r = 1$, so $r = 0$. (1 point)

2. Let $s, r \in \mathbb{Z}_+$ and let $s \geq 1$. Prove that $(p^{sr} - 1)/(p^s - 1) \equiv r \bmod p^s - 1$.
Solution: $(p^{sr} - 1)/(p^s - 1) = p^{s(r-1)} + p^{s(r-2)} + \ldots + p^s + 1$ and $p^s \equiv 1 \bmod p^s - 1$, hence the result follows. (1 point)

3. Prove that the relation $m = nk$ is Diophantine over $\mathbb{N}$ in the language $L_0 = \{0, 1, +, /_p, P, t\}$.
Solution: In the lecture we proved that the relation $m = p^s n$ is Diophantine over $\mathbb{N}$ in L_0. We have also proven that $m = n^2$ if and only if

$$\begin{gathered}\exists s, r \in \mathbb{Z}_+((p^{2s} - 1)/(p^r - 1), (p^r - 1)/(p^{2s} - 1) \equiv n \bmod p^{2s} - 1, n < p^s - 1, \\ ((p^r - 1)/(p^{2s} - 1))^2 \equiv m \bmod p^{2s} - 1 \text{ and } m < p^{2s} - 1).\end{gathered}$$

We can find a Diophantine expression in L_0 equivalent to this, since $m = p^s n$ is Diophantine and

$$\begin{gathered}(p^{2s} - 1)|(p^r - 1) \Leftrightarrow \\ \exists x(xp^{2s} - x = p^r - 1), \\ (p^r - 1)/(p^{2s} - 1) \equiv n \bmod p^{2s} - 1 \Leftrightarrow \\ \exists k \in \mathbb{Z}_+((p^r - 1) = (k(p^{2s} - 1) + n)(p^{2s} - 1)), \\ n < p^s - 1 \Leftrightarrow \\ \exists a(n + a + 1 = p^s - 1), \\ (p^x - 1)^2 \Leftrightarrow \\ \exists k(m = k(p^x - 1) \wedge k = p^x - 1).\end{gathered}$$

Hence the relation $m = n^2$ is Diophantine in L_0. (3 points) We have that $m = nk$ if and only if $(n + k)^2 = n^2 + 2m + k^2$, hence $m = nk$ is Diophantine over $\mathbb{N}$ in L_0. (1 point)

4. We have proven that the existential problem for $F[[t]]$ in the language $L = \{0, 1, +, \cdot, P, t\}$ is undecidable. Prove that for a ring R such that $F[t] \subset R \subset K((t))$, the existential problem for R in the language L is undecidable too.
Solution: Undecidability for $F[[t]]$ followed from coding the Diophantine problem for $\mathbb{N}$ and $/_p$ into the existential problem for $F[[t]]$ and $\cdot$. We can use the same definitions for R. (2 points) (The goal of this exercise was not necessarily to give a very detailed answer but to go over the whole proof once again.)