Theory of Computation

Homework 4

Due: 2013/12/10

Problem 1. Determine if $x^4 \equiv 25 (\text{mod } 1013)$ is solvable or not.

Solution.

Let's first notice that 1013 is a prime. Since 25 has square roots ± 5, we need to check if any of the Legendre symbols $\left(\frac{5}{1013}\right)$ or $\left(\frac{-5}{1013}\right)$ is 1, so calculating we have

$$\left(\frac{5}{1013}\right) = \left(\frac{1013}{5}\right) = \left(\frac{3}{5}\right) = -1$$

and

$$\left(\frac{-5}{1013}\right) = \left(\frac{-1}{1013}\right)\left(\frac{5}{1013}\right) = (-1)^{\frac{1013-1}{2}}\left(\frac{5}{1013}\right) = \left(\frac{5}{1013}\right) = -1$$

so 25 is not a quadratic residue modulo 1013, hence it cannot be a solution of $x^4 \equiv 25 (\text{mod } 1013)$. $\square$

Problem 2. Prove that if $\mathbf{NP} \subseteq \mathbf{coRP}$, then $\mathbf{ZPP} = \mathbf{NP}$

Solution.

We know that $\mathbf{RP} \subseteq \mathbf{NP}$ and by hypothesis $\mathbf{NP} \subseteq \mathbf{coRP}$, so

$$\mathbf{RP} \subseteq \mathbf{NP} \subseteq \mathbf{coRP}$$

and because $\mathbf{coRP} \subseteq \mathbf{coNP}$, we get that

$$\mathbf{RP} \subseteq \mathbf{NP} \subseteq \mathbf{coRP} \subseteq \mathbf{coNP}$$

Now, because $\mathbf{NP} \subseteq \mathbf{coRP}$, then $\mathbf{coNP} \subseteq \mathbf{RP}$, so using this in the last chain we get

$$\mathbf{coNP} \subseteq \mathbf{RP} \subseteq \mathbf{NP} \subseteq \mathbf{coRP} \subseteq \mathbf{coNP}$$

Hence $\mathbf{coNP} = \mathbf{RP} = \mathbf{NP} = \mathbf{coRP}$. Finally, let's notice that

$$\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP} = \mathbf{NP} \cap \mathbf{NP} = \mathbf{NP}$$

showing what was requested. $\square$