Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Tutorial 1
- Proposed Solution -

Friday, October 30, 2015

Solution of Problem 1

"⇒" c is QR modulo p with Definition 9.1 it follows

$$\exists\, x \in \mathbb{Z}_p^* : x^2 \equiv c \mod p \Rightarrow c^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p,$$

where the last congruence follows from Fermat's Theorem.

"⇐" $c^{\frac{p-1}{2}} \equiv 1 \mod p \Rightarrow c \in \mathbb{Z}_p^*$ as c has an inverse modulo p.
Let y be a primitive element (PE), i.e., y is a generator of $\mathbb{Z}_p^*$. Note that there exists a primitive element with respect to Theorem 7.2 a).

$$\begin{aligned}
&\Rightarrow && \exists\, j : c \equiv y^j \mod p \\
&\Rightarrow && c^{\frac{p-1}{2}} \equiv (y^j)^{\frac{p-1}{2}} \equiv 1 \mod p \\
&\Rightarrow && p-1 \mid j(p-1)/2 \Rightarrow j \text{ must be even} \\
&\Rightarrow && \exists\, x \in \mathbb{Z}_p^* : x \equiv y^{\frac{j}{2}} \mod p \\
&\Rightarrow && x^2 \equiv y^j \equiv c \mod p \\
&\Rightarrow && c \text{ is QR modulo } p
\end{aligned}$$

Solution of Problem 2

This problem is usually a difficult problem, but we can solve it, because 31 is prime. First, apply Proposition 7.5 to show that 17 is a primitive element modulo 31.

$$\begin{aligned}
17^{\frac{p-1}{p_i}} &\overset{!}{\not\equiv} 1 \mod p \quad \forall i = 1, \ldots, k, \quad \text{where } p-1 = \prod_{i=1}^{k} p_i^{t_i} \\
p = 31 \Rightarrow p-1 &= 30 = 2 \cdot 3 \cdot 5 \\
17^{\frac{30}{2}} &\equiv 30 \not\equiv 1 \mod 31 \\
17^{\frac{30}{3}} &\equiv 25 \not\equiv 1 \mod 31 \\
17^{\frac{30}{5}} &\equiv 8 \not\equiv 1 \mod 31
\end{aligned}$$

17 is a primitive element modulo 31 and we can conclude:

$$\begin{aligned}
\exists b : 17^b &\equiv a \mod 31 \\
(a^{13})^b &\equiv a \mod 31 \\
a^{13 \cdot b - 1} &\equiv 1 \mod 31
\end{aligned}$$

With Fermats little theorem (Theorem 6.2, let $a \in \mathbb{Z}_n^*$, then $a^{\varphi(n)} \equiv 1 \mod n$), we can say:

$$\begin{aligned}
a^{\varphi(n)} &\equiv a^{30} \equiv 1 \mod 31 \\
a^{13 \cdot b - 1} &\equiv a^{30} \equiv 1 \mod 31 \\
\Rightarrow 13 \cdot b - 1 &\equiv 30 \mod 30 \\
13 \cdot b &\equiv 1 \mod 30 \\
b &\equiv 13^{-1} \mod 30
\end{aligned}$$

The Extended Euclidean Algorithm yields $13 \cdot 7 - 30 \cdot 3 = 1$ and thus $b = 13^{-1} \equiv 7 \mod 30$. It remains to compute $a \equiv 17^b \equiv 17^7 \equiv 12 \mod 31$.