Quiz 5 Solutions

Tim Smits

1. Let $a, n \in \mathbb{N}$ with $a > 1$.

(a) Prove that $\text{ord}_{a^n-1}(a) = n$.

(b) Deduce that $n \mid \varphi(a^n - 1)$.

Solution:

(a) Note that $a^n - 1 \equiv 0 \bmod a^n - 1$, so that $a^n \equiv 1 \bmod a^n - 1$. Suppose that $a^d \equiv 1 \bmod a^n - 1$ for $1 < d < n$. This says $a^n - 1 \mid a^d - 1$, which is clearly not possible. Therefore, $\text{ord}_{a^n-1}(a) = n$.

(b) Since $a^{\varphi(a^n-1)} \equiv 1 \bmod a^n - 1$ and $\text{ord}_{a^n-1}(a) = n$, we immediately see that $n \mid \varphi(a^n - 1)$.

2. Solve the following system of congruences:

$$\begin{cases} x \equiv 7 \bmod 12 \\ x \equiv 3 \bmod 10 \\ x \equiv 13 \bmod 18 \end{cases}$$

Solution: From the first equation, $x = 7 + 12k$ for some $k \in \mathbb{Z}$. Plug into the second equation, so that $7 + 12k \equiv 3 \bmod 10$ says $2k \equiv 6 \bmod 10$, i.e. $2k = 6 + 10m$ for some $m \in \mathbb{Z}$. This says $k = 3 + 5m$, so $x = 43 + 60m$. Plugging into the third equation says $43 + 60m \equiv 13 \bmod 18$, so that $6m \equiv 6 \bmod 18$. This says $6m = 6 + 18\ell$ for some $\ell \in \mathbb{Z}$, so that $m = 1 + 3\ell$. This gives $x = 103 + 180\ell$, so that $x \equiv 103 \bmod 180$.