Blatt 4

Aufgabe I :

Let w be a primitive root modulo p, s.t.

$$w^{p-1} \not\equiv 1 \mod p^2,$$

i.e.

$$w^{p-1} = 1 + pt \quad , \quad p \nmid t .$$

The mentioned proof concludes then via induction that

$$w^{(p-1)p^{n-1}} = 1 + p^n t_n \quad \text{with} \quad p \nmid t_n$$

(which implies then that the order of w mod p^{n+1} equals $\varphi(p^{n+1}) = p^n(p-1)$.

In the induction step $n \longmapsto n+1$ one writes

$$w^{(p-1)p^n} = w^{(p-1)p^{n-1} \cdot p} = (1 + p^n t_n)^p$$
$$= 1 + \binom{p}{1} p^n t_n + \binom{p}{2} (p^n t_n)^2 + \dots$$
$$= 1 + p^{n+1} t_{n+1},$$

where $t_{n+1} \equiv t_n \mod p$, i.e. $p \nmid t_{n+1}$.

However for $p=2$ we have

$$w^{(p-1)p^n} = (1 + p^n t_n)^2 = 1 + 2^{n+1} t_n + 2^{2n} t_n^2$$
$$= 1 + 2^{n+1} (t_n + 2^{n-1} t_n^2),$$

and for $n=1$ we find $t_n + 2^{n-1} t_n^2 \equiv 0 \mod 2$.

Aufgabe II:

We show by induction that

(*) $\operatorname{ord}(5 \bmod 2^n) = 2^{n-2} \quad (n \geq 3)$.

This implies then the claim. Namely, let a be odd. Choose $\varepsilon \in \{\pm 1\}$ s.t. $a' := \varepsilon a \equiv 1 \bmod 4$. Then for $n \geq 3$, $a' \bmod 2^n \in U_n := \{\rho \in (\mathbb{Z}/2^n\mathbb{Z})^\times : \rho \equiv_4 +1\}$. But $\#U_n = 2^{n-2}$ and $5 + 2^n\mathbb{Z} \in U_n$, i.e. $U_n = \langle 5 + 2^n\mathbb{Z} \rangle$ by (*). It follows

$a' \equiv 5^t \bmod 2^n$ for some t, and this is the claim.

For (*) proceed by induction. $n=3$ is clear. The step $n \longmapsto n+1$ is as follows:

$\operatorname{ord}(5 \bmod 2^n) = 2^{n-2}$ by induction hypothesis

i.e.

$$5^{2^{n-3}} = 1 + 2^{n-1} t \quad \text{with odd } t.$$

But then

$$5^{2^{n-2}} = (1 + 2^{n-1}t)^2 = 1 + 2^n t + 2^{2n-2} t^2 \not\equiv 1 \bmod 2^{n+1},$$

which implies

$$\operatorname{ord}(5 + 2^{n+1}\mathbb{Z}) = 2^{n-1} \qquad \square$$