DS_2013 $\qquad$ <u>Corrigé</u>.

1) Comme $\mathbb{F}_p[x]$ est de caractéristique p,

$$Q^p = \left(\sum_{i=0}^{n} q_i x^i\right)^p = \sum_{i=0}^{n} q_i^p x^{pi}.$$

Comme $q_i \in \mathbb{F}_p$ pour tout i, $q_i^p = q_i$, donc

$$Q^p = \sum_{i=0}^{n} q_i x^{pi}.$$

2) Si $R = Q^p$, $R' = pQ'Q^{p-1} = 0$.

Si $R' = 0$, on écrit $R = \sum_{i=0}^{d} r_i x^i$ et donc $R' = \sum_{i=1}^{d} r_i i x^{i-1}$. Ainsi, pour tout i, $i r_i = 0$ et donc, si p ne divise pas i, $r_i = 0$.

Ainsi, $R = \sum_{i=0}^{d'} r_{pi} x^{pi} = \left(\sum_{i=0}^{d'} r_{pi} x^i\right)^p$.

3) $\operatorname{pgcd}(P, P') = \prod_{i=1}^{r} P_i^{v_i}$, où pour tout i, v_i est le plus grand entier inférieur ou égal à e_i tel que $P_i^{v_i}$ divise P'.

$$P' = \sum_{i=1}^{r} e_i P_i' P_i^{e_i-1} \prod_{j\neq i} P_j^{e_j} = \sum_{i\in I} e_i P_i' P_i^{e_i-1} \prod_{j\neq i} P_j^{e_j}.$$

Donc pour tout i dans J, $P_i^{e_i}$ divise P', et pour tout i dans I, $P_i^{e_i-1}$ divise P'. Reste à voir que si $i \in I$, $P_i^{e_i}$ ne divise pas P'.

$$P' = e_i P_i' P_i^{e_i-1} \prod_{j\neq i} P_j^{e_j} + \sum_{k\in I\setminus\{i\}} e_k P_k' P_k^{e_k-1} \prod_{j\neq k} P_j^{e_j}.$$

$P_i^{e_i}$ divise le second terme de cette somme, mais pas le premier. Donc $P_i^{e_i}$ ne divise pas P'. On en déduit que $\operatorname{pgcd}(P, P') = \prod_{i\in I} P_i^{e_i-1} \prod_{j\in J} P_j^{e_j}$.

Donc : $U = \prod_{i\in I} P_i$ et $V = \dfrac{\prod P_i^{e_i}}{\prod_{i\in I} P_i^{e_i}} = \prod_{j\in J} P_j^{e_j}$.

4) $V = \left(\prod_{j\in J} P_j^{e_j/p}\right)^p$ (en effet, pour tout j dans J, p divise e_j).

5) $P = x^{11} + x^{10} + 2x + 2$, $P' = x^{10} + 2$, $\operatorname{pgcd}(P, P') = x^{10} + 2$, $U = x + 1$,
$V = x^{10} + 2$, $W = x^2 + 2$, $\operatorname{PSFC}(P) = (x+1)(x^2+2)$.

7) Si $q = p^k$ et si $\alpha \in \mathbb{F}_q$, $\alpha^q = \alpha$. Donc $\left(\alpha^{p^{k-1}}\right)^p = \alpha$.
Ainsi, la racine p^e de α est $\alpha^{p^{k-1}}$.

Si $V = x^{12} + (a^2+1)x^6 + (a+2)x^3 + a \in \mathbb{F}_{27}[x]$,

$$W = x^4 + (a^2+1)^9 x^2 + (a+2)^9 x + a^9 = x^4 + (a^2+2a+2)x^2 + ax + a + 1.$$