

# NMAG436 - HW4

Jan Oupický

## 1

Let  $L := \mathbb{F}_p(V_{w_a})$ .  $w_a$  is a short WEP by definition for every  $p$  and  $a$ .

First let  $p = 2$ :

$w_0 = y^2 + x^3, w_1 = y^2 + x^3 + 1$  with partial derivatives  $\frac{\partial w_0}{\partial x}(x, y) = x^2, \frac{\partial w_0}{\partial y}(x, y) = 0, \frac{\partial w_1}{\partial x}(x, y) = x^2, \frac{\partial w_1}{\partial y}(x, y) = 0$ . We see that  $V_{w_0}(\mathbb{F}_2) = \{(0, 0), (1, 1)\}, V_{w_1}(\mathbb{F}_2) = \{(1, 0), (0, 1)\}$ . We see that  $w_0$  is not smooth at  $(0, 0)$  and  $w_1$  at  $(0, 1)$  therefore they are not smooth.

Theorem 8.4 tells us that  $L$  is an EFF iff  $w$  is smooth therefore  $L$  is not an EFF. Proposition 8.3 5) tells us that the only other option is that the genus of  $L$  is 0.

Now let  $p > 2$ :

Let  $f := x^3 + a \in \mathbb{F}_p[x]$ . We want to know for which  $a$  is  $f$  separable. By definition we want to know when  $\text{GCD}_{\mathbb{F}_p[x]}(f, f') = 1$ . Since  $f' = 3x^2$  for every  $a$ , we can see that  $f, f'$  are not coprime iff  $a = 0$  (if  $p = 3$  then  $f' = 0$  and still:  $f$  is separable iff  $a \neq 0$ ). From that we see:

If  $a = 0$  then  $w_a$  is not smooth by 3.12. 3) which implies that the genus of  $L$  is 0 (same reasoning as in the case  $p = 2$ ).

If  $a \neq 0$  then  $w_a$  is smooth and by 8.4 the genus of  $L$  is 1.

## 2

Let  $L = \mathbb{F}_5(V_w)$  (i.e.  $L$  is given by  $w(\alpha, \beta) = 0$  where  $\alpha = x + (w), \beta = y + (w)$ ).

We calculate the partial derivatives of  $w$ :  $\frac{\partial w}{\partial x}(x, y) = y - 3x^2 + 1, \frac{\partial w}{\partial y}(x, y) = 2y + x$ . By substituting the point  $(1, 2)$  we get that both derivatives are equal to 5 which is 0 since we are in  $\mathbb{F}_5$ . Therefore  $w$  is singular at  $(1, 2)$ .

Now we need a shifted polynomial which gives us the same  $L$ . As in previous exercises we use translation  $\tau_\gamma$  given by a vector  $\gamma := (1, 2)$ . We denote the new polynomial which is singular at  $(0, 0)$  by  $w'$ . As before  $w' := \tau_\gamma^*(w) = w(x + 1, y + 2) = y^2 + xy + 4x^3 + 2x^2$  and also we get elements  $(u, t) = \tau_{-\gamma}(\alpha, \beta) = (\alpha - 1, \beta - 2)$  (following the proof of 5.8, 5.5 and 3.10). Now we now that  $L$  is also given by  $w'(u, t) = 0$ .

We have now satisfied the conditions assumed in the one implication in proof of 8.4 and we can follow it. So we define  $s := \frac{t}{u}$ . As in the proof we know  $w'(u, t) = 0 \implies \frac{w'(u, t)}{u^2} = 0 \implies 0 = s^2 + s - u + 2 \iff u = s^2 + s + 2 \in \mathbb{F}_5(s)$  and from the definition of  $s$  we get  $t = su = s(s^2 + s + 2) \in \mathbb{F}_5(s)$ . Which means that  $L = \mathbb{F}_5(\alpha, \beta) = \mathbb{F}_5(u, t) = \mathbb{F}_5(s)$ .

But from the definitions:  $s = \frac{t}{u} = \frac{\alpha - 1}{\beta - 2} = \frac{x - 1 + (w)}{y - 2 + (w)} \in L$  we see that the element we are looking for is  $\in \mathbb{F}_5(x, y)$  therefore we let  $s$  be actually  $\frac{x-1}{y-2}$ .

### 3

Let  $L = \mathbb{F}_5(V_f)$  (i.e.  $L$  is given by  $f(\alpha, \beta) = 0, \alpha = x + (f), \beta = y + (f)$ ) where  $f = y^2 - (x^3 - 2) \in \mathbb{F}_5[x, y]$  and denote  $\bar{f} := (x^3 - 2)$ . We see that  $f$  is a (short) WEP therefore absolutely irreducible by 4.9. By calculating  $\bar{f}' = 3x^2$  and  $\text{GCD}_{\mathbb{F}_5[x]}(\bar{f}, \bar{f}') = 1$  we see that  $\bar{f}$  is separable in  $\mathbb{F}_5[x]$  therefore  $f$  is smooth (at  $V_f$ ). We have satisfied the assumptions of theorem 8.4 and so we have proved that  $L$  is EFF.

- (a) Using definition of  $E := E(\mathbb{F}_5) = V_f(\mathbb{F}_5) \cup \{\infty\}$  we have to find all roots of  $f$  in  $\mathbb{F}_5$  so thats (25 combinations).

We calculate that  $V_f(\mathbb{F}_5) = \{(1, 2), (1, 3), (2, 1), (2, 4), (3, 0)\} \implies E = \{(1, 2), (1, 3), (2, 1), (2, 4), (3, 0), \infty\}$ . We know that  $E$  is finite and an abelian group therefore is it cyclic (and therefore isomorphic to  $\mathbb{Z}_6$ ). By Lagrange theorem we know that  $E$  can have elements only of orders 1 (neutral element which is  $\infty$  by definition of  $E$ ), 2, 3 and 6 (a generator). We want to look for  $\gamma \in V_f(\mathbb{F}_5)$  such that  $\gamma \oplus \gamma \neq \infty$  (not of order 2) and  $\gamma \oplus \gamma \neq \ominus \gamma \iff \gamma \oplus \gamma \oplus \gamma = \infty$  (not of order 3).

If we straight up use the formulas given by theorem 8.8 (where  $a_1 = a_2 = a_3 = a_4 = 0, a_6 = -2 = 3$ ) we see that  $\gamma = (1, 2)$  is of order 6 since:

$$\begin{aligned} \text{using 8.8 1): } \ominus \gamma &= (1, -2) = (1, 3) \implies \gamma \neq \ominus \gamma \\ \delta &:= \gamma \implies \gamma \neq \ominus \delta \text{ assumption of 2)} \\ \text{using 8.8 2): } \mu &= \gamma \oplus \gamma \\ \lambda &:= \frac{3 \cdot (1)^2}{2 \cdot 2} = \frac{3}{4} = \frac{3}{-1} = -3 = 2 \\ \implies \mu_1 &= -1 - 1 + 2^2 = -2 + 4 = 2 \\ \implies \mu_2 &= 2(1 - 2) - 2 = -2 - 2 = -4 = 1 \implies \\ \gamma \oplus \gamma &= (2, 1) \neq \infty, \ominus \gamma \end{aligned}$$

Therefore  $(1, 2)$  is a generator.

- (b) Let  $D := \sum_{\gamma \in E(\mathbb{F}_5)} 1P_\gamma$ . By definition  $\deg(D) = \sum_{\gamma \in E(\mathbb{F}_5)} 1\deg_{\mathbb{F}_5}(P_\gamma)$ . Since we have shown that  $w$  is smooth then by 8.3 4) we know that  $\deg_{\mathbb{F}_5}(P_\gamma) = 1, \forall \gamma \in E(\mathbb{F}_5)$ . We have shown that  $L$  is EFF that means  $L$  is full constant and genus is 1. So we can use Corollary 7.6 2) since  $6 \geq 2 - 1 = 1 \implies l(D) = \deg(D) + 1 - 1 = 6$ . By definition  $l(D) = \dim_{\mathbb{F}_5}(\mathcal{L}(D))$  so the  $\mathbb{F}_5$ -dimension of  $R$  is 6.

Using lemma 6.2 where  $A := \underline{0}, B := D$  ( $D \geq \underline{0}$  by definition) we get that  $\mathcal{L}(\underline{0}) \subseteq \mathcal{L}(D)$ . Using observation B 5) we get that  $\mathcal{L}(\underline{0}) = \tilde{\mathbb{F}}_5 \stackrel{L \text{ is full constant}}{=} \mathbb{F}_5$ . Therefore we can see that for example 2 is a nonzero element of  $\mathbb{F}_5 \subseteq R$ .