

Elliptic Curves MT25: Solutions to Sheet 3

- (1) Following the hint, there exist polynomials $p(x), q(x) \in R[x]$ such that $p(x)f(x) + q(x)f'(x) = D$, and so: $p(a_0)f(a_0) + q(a_0)f'(a_0) = D$. Since $|a_0| \leq 1$, and since $p(x), q(x), f(x), f'(x) \in R[x]$, we must have

$$|p(a_0)|, |f(a_0)|, |q(a_0)|, |f'(a_0)| \leq 1$$

and so $|D| \leq \max(|p(a_0)f(a_0)|, |q(a_0)f'(a_0)|) \leq 1$, which also implies $|D^2| = |D|^2 \leq |D|$. Now, we are given that $|f(a_0)| < |D|^2$ and so $|p(a_0)f(a_0)| \leq |f(a_0)| < |D|^2 \leq |D|$. Hence $|D| \neq |p(a_0)f(a_0)|$, and so $|q(a_0)f'(a_0)| = |D - p(a_0)f(a_0)| = \max(|D|, |p(a_0)f(a_0)|) = |D|$ [using the fact that, if $|u| \neq |v|$ then $|u \pm v| = \max(|u|, |v|)$]. Since also $|q(a_0)| \leq 1$, this gives that $|f'(a_0)| \geq |D|$. Finally, $|f(a_0)| < |D|^2 \leq |f'(a_0)|^2$, and so $f(X)$ has a root $a \in R$ by Hensel's Lemma.

- (2) In projective form, the point is: $(-64/25, 59/125, 1)$. The coordinate with largest 5-adic value is $59/125$, and on dividing all coordinates through by this, we can also represent the point as: $(-320/59, 1, 125/59)$, which is in 5-adic standard form (that is, 1 is the maximum of the 5-adic valuations of the coordinates). Reducing mod 5 gives $(0, 1, 0)$ on $\tilde{\mathcal{E}}$, which is the point at infinity.

- (8) Take $F(X, Y) = X + Y + tXY^p$, clearly non-commutative. One only has to check associativity.

$$\begin{aligned} F(F(X, Y), Z) &= F(X + Y + tXY^p, Z) = X + Y + tXY^p + Z + t(X + Y + tXY^p)Z^p \\ &= X + Y + tXY^p + Z + tXZ^p + tYZ^p, \end{aligned}$$

since the remaining term $t^2XY^pZ^p \in I = t^2\mathbb{F}_p[t]$ and so $t^2XY^pZ^p = 0$ in $R = \mathbb{F}_p[t]/I$. Also:

$$\begin{aligned} F(X, F(Y, Z)) &= X + F(Y, Z) + tXF(Y, Z)^p = X + Y + Z + tYZ^p + tX(Y + Z + tYZ^p)^p \\ &= X + Y + Z + tYZ^p + tX(Y^p + Z^p + (tYZ^p)^p), \end{aligned}$$

since all other terms in the binomial expansion of $(Y + Z + tYZ^p)^p$ are divisible by p and so are equal to 0 in R , which has characteristic p . But $(tYZ^p)^p = t^p(t^{p-2}Y^pZ^{p^2}) \in I$ and so $(tYZ^p)^p = 0$ in R , so that the above are the same, giving associativity, as required.

- (9) Hint: consider the order 4 automorphism (of elliptic curves over $\mathbb{C}$) $(x, y) \mapsto (-x, iy)$. This induces an automorphism of the formal group associated to $Y^2 = X^3 + AX$.

See the full solutions file for the full solution!

- (10) First we show convergence of the right hand side. For each i , set $g_i = G_i(x_1, \dots, x_l)$. We have $|g_i| \leq \max(|x_i|) < 1$. Choose $\rho < 1$ such that $\max(|x_i|) = \rho\delta$ with $\delta < 1$. Since $\{|a_n|\rho^{\sum n_i}\}$ is bounded, say by C , we have

$$\left| \sum_{n: \sum n_i \geq N} a_n g_1^{n_1} \dots g_k^{n_k} \right| \leq C\delta^N.$$

It follows that the right hand side converges, and is the limit of the sequence

$$\sum_{n: \sum n_i \leq N-1} 1 \cdot a_n g_1^{n_1} \dots g_k^{n_k}$$

as $N \rightarrow \infty$.

Write $G_i = \sum b_{i,m} X_1^{m_1} \dots X_l^{m_l}$ and for a positive integer M consider the finite truncations $G_{i,M} = \sum_{\sum m_i \leq M-1} b_{i,m} X_1^{m_1} \dots X_l^{m_l}$ with values $g_{i,M}$ when we substitute the x_i .

We have