Elliptic Curves Example Sheet 2

Isaac Martin

Last compiled February 23, 2022

EXERCISE 1. Find all points defined over the field $\mathbb{F}_{13}$ of 13 elements on the elliptic curve

$$y^2 = x^3 + x + 5$$

and show that they form a cyclic group. Find an example of an elliptic curve over $\mathbb{F}_{13}$ for which this group is not cyclic. Are there any examples where the group requires more than two generators?

> *Proof:* By brute force (i.e. a Python script) one can check that
>
> $$E(\mathbb{F}_{13}) = \{O_E, (1,10), (2,7), (3,3), (4,12), (9,12), (10,3), (11,7), (12,10)\}.$$
>
> Counting, this means that $\#E(\mathbb{F}_{13}) = 9$. There are two groups of order 9, $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. One can choose any non-identity point in $E(\mathbb{F}_{13})$ and add it to itself three times to verify that it is not order 3, and must therefore be order 9. Hence this is cyclic.
>
> I didn't finish this question. □

EXERCISE 2. Let A be an abelian group and let $q : A \to \mathbb{Z}$ be a map satisfying

$$q(x+y) + q(x-y) = 2q(x) + 2q(y).$$

Prove that A is a quadratic form.

> *Proof:* Recall that to be a quadratic form, q must satisfy
>
> (i) $q(nx) = n^2 q(x)$ for all $x \in A$ and $n \in \mathbb{Z}$
>
> (ii) $\langle x, y\rangle = q(x+y) - q(x) - q(y)$ is a $\mathbb{Z}$-bilinear pairing.
>
> We prove these properties by induction.
>
> **(i)** Notice that $q(1 \cdot x) = 1^2 q(x)$ trivially, $q(0+0) + q(0-0) = 2q(0) + 2q(0)$ so $q(0) = 0$, and $q(2x) = 2q(x) + 2q(x) - q(x-x) = 4q(x)$ for all $x \in A$; hence, (i) holds for $n = 0, 1$ and 2. Now suppose that (i) holds for all positive values k with $n > k > 2$. By induction,
>
> $$\begin{aligned} q(nx) &= 2q((n-1)x) + 2q(x) - q((n-2)x) \\ &= 2(n-1)^2 q(x) + 2q(x) - (n-2)^2 q(x) \\ &= (2n^2 - 4n + 2 + 2 - n^2 + 4n - 4)q(x) = n^2 q(x), \end{aligned}$$
>
> so (i) holds for all values $n \geq 0$.

Finally, if $n \geq 0$ then

$$\begin{aligned}
q(-nx) &= q(x-(n+1)x) = 2q(x) + 2q((n+1)x) - q(x+(n+1)x) \\
&= 2q(x) + 2(n+1)^2 q(x) - (n+2)^2 q(x) \\
&= (2 + 2n^2 + 4n + 2 - n^2 - 4n - 4)q(x) = n^2 q(x).
\end{aligned}$$

This means $q(nx) = n^2 q(x)$ for all $n \in \mathbb{Z}$ and $x \in A$.

(ii) Since the pairing $\langle x, y\rangle$ is invariant under the permutation $x \mapsto y$ and $y \mapsto x$, it suffices to prove that $\langle -, -\rangle$ is $\mathbb{Z}$-linear in the first coordinate, i.e. that

(a) $\langle nx, y\rangle = n\langle x, y\rangle$ for all $n \in \mathbb{Z}$ and $x, y \in A$

(b) $\langle x+y, z\rangle = \langle x, y\rangle + \langle y, z\rangle$ for all $x, y, z \in A$.

(a) We first treat the case that $n \geq 0$. This induction argument requires that the statement hold true for $n-1, n-2$ and $n-3$, so we need the cases that $n = 0, 1$ and 2 before proceeding to the induction step.

$\underline{n=0}$: $\langle 0\cdot x, y\rangle = q(0\cdot x + y) - q(0\cdot x) - q(y) = q(y) - q(y) = 0 = 0\cdot\langle x, y\rangle$.

$\underline{n=1}$: This is trivially satisfied.

$\underline{n=2}$: We invoke the equality $q(2x) = 4q(x)$ provided by (i) here.

$$\begin{aligned}
\langle 2x, y\rangle &= q(2x+y) - q(2x) - q(y) \\
&= q(x + (x+y)) - q(2x) - q(y) \\
&= 2q(x) + 2q(x+y) - q(x-(x+y)) - 4q(x) - q(y) \\
&= 2q(x+y) - 2q(x) - q(-y) - q(y) \\
&= 2\big(q(x+y) - q(x) - q(y)\big) = 2\langle x, y\rangle.
\end{aligned}$$

Assume now that $n > 2$ and that $\langle kx, y\rangle = k\langle x, y\rangle$ holds for $n > k \geq 0$. This means

$$\langle kx, y\rangle = q(kx+y) - q(kx) - q(y) = k\big(q(x+y) - q(x) - q(y)\big)$$

for $0 \leq k < n$ and so

$$\begin{aligned}
q(kx+y) &= k\big(q(x+y) - q(x) - q(y)\big) + k^2 q(x) + q(y) \qquad (*) \\
&= kq(x+y) + (k^2-k)q(x) - (k-1)q(y).
\end{aligned}$$

We can now prove the desired statement:

$$
\begin{aligned}
\langle nx, y\rangle &= q(nx+y)-q(nx)-q(y) \\
&= 2q(x)+2q\big((n-1)x+y\big)-q\big((n-2)x+y\big)-q(nx)-q(y) \\
&= 2q(x)+\overbrace{2(n-1)(q(x+y)+2(n-1)(n-2)q(x)-2(n-2)q(y))}^{2q\left((n-1)x+y\right)\text{ by }(*)} \\
&\quad -\overbrace{(n-2)q(x+y)-(n-2)(n-3)q(x)+(n-3)q(y)}^{-q\left((n-2)x+y\right)\text{ by }(*)}-n^2q(x)-q(y) \\
&= \big(2(n-1)-(n-2)\big)q(x+y)+\big(2+2(n-1)(n-2)-(n-2)(n-3)-n^2\big)q(x) \\
&\quad +\big(-2(n-2)+(n+3)-1\big)q(y) \\
&= nq(x+y)-nq(x)-nq(y) \\
&= n\langle x,y\rangle .
\end{aligned}
$$

We now must treat the case that $n<0$. If $n=-1$ we get

$$
\begin{aligned}
\langle -x, y\rangle &= q(-x+y)-q(-x)-q(y) \\
&= 2q(x)+2q(y)-q(x+y)-q(x)-q(y)=-\langle x,y\rangle
\end{aligned}
$$

without too much trouble. Using this together with the $n \geq 0$ case gives us

$$\langle -nx, y\rangle = -\langle nx, y\rangle$$

for $n \geq 0$, so we conclude that $\langle nx, y\rangle = n\langle x, y\rangle$ for all $n \in \mathbb{Z}$.

(b) Let $x,y,z \in A$ be arbitrary elements. By expanding $\langle -,-\rangle$ it can be seen that

$$\langle x+y, z\rangle - \langle x, z\rangle - \langle y, z\rangle = 0$$

if and only if

$$q(x+y+z)=q(x+y)+q(x+z)+q(y+z)-q(x)-q(y)-q(z).$$

We prove this later equality. We first examine what we obtain by considering $q(x+y+z)$ and swapping each "+" one at a time. By assumption, we have that

$$q(x+y+z)+q(x+y-z)=2q(x+y)+2q(z), \tag{1}$$

$$q(x+y-z)+q(x-y-z))=2q(x-z)+2q(y) \tag{2}$$

and

$$q(x-y-z)+q(-x-y-z)=2q(-y-z)+2q(x). \tag{3}$$

Adding equations (1) and (3) together and subtracting equation (2) gives us

$$q(x+y+z)+q(-x-y-z)=2q(x+y)+2q(z)-2q(x-z)-2q(y)+2q(y+z)+2q(x),$$

while recalling that $q(-x) = q(x)$, dividing both sides by 2 and performing some convenient rearranging gives us

$$q(x+y+z) = \big[q(x+y)q(y+z) - q(y)\big] + \big[q(x-z) + q(z) + q(x)\big].$$

Finally, we have that $q(x-z) = 2q(x) + 2q(z) - q(x+z)$. Substituting this in for $q(x-z)$, combining like terms, and rearranging a final time yields

$$q(x+y+z) = q(x+y) + q(x+z) + q(y+z) - q(x) - q(y) - q(z)$$

as desired. $\square$

EXERCISE 3. Find a translation-invariant differential ω on the multiplicative group $\mathbb{G}_m$. Show that if $[n] : \mathbb{G}_m \to \mathbb{G}_m$ is the endomorphism $x \mapsto x^n$ then $[n]^* \omega = n\omega$.

Proof: An invariant differential of a formal group law $F \in R[\![X,Y]\!]$ is a differential form

$$\omega = P(T)dT \in R[\![T]\!]dT$$

which satisfies

$$\omega \circ F(T,S) = \omega(T)$$
$$\iff$$
$$P(F(T,S))F_X(T,S) = P(T)$$

where $F_X(T,S)$ is the partial derivative of F in the first variable. The formal group law of $\mathbb{G}_m$ is $F(X,Y) = X+Y+XY = (1+X)(1+Y) - 1$, and its partial derivative in X is $F_X(X,Y) = 1+Y$. We are therefore looking for some $P(T) \in R[\![T]\!]$ such that

$$P((1+T)(1+S)-1) \cdot (1+S) = P(T).$$

It is fortunate that we discussed the element $\frac{1}{1-X} = 1 + x + x^2 + \ldots \in R[\![T]\!]$ in class – a slight modification, the power series $P(T) = \frac{1}{1+T} = 1 - T + T^2 - T^3 + \ldots \in R[\![T]\!]$, will do the trick:

$$P((1+T)(1+S)-1) \cdot (1+S) = \frac{1}{(1+T)(1+S)-1+1} \cdot (1+S) = \frac{1}{1+T} = P(T).$$

Hence the differential form $\omega = \frac{1}{1+T}$ is an invariant differential of the multiplicative formal group law. $\square$

EXERCISE 6. Show that if $\phi \in \mathrm{End}(E)$ then there exists $\mathrm{tr}(\phi) \in \mathbb{Z}$ such that

$$\deg([n] + \phi) = n^2 + n\,\mathrm{tr}(\phi) + \deg(\phi)$$

for all $n \in \mathbb{Z}$. Establish the following properties:

(i) $\mathrm{tr}(\phi + \psi) = \mathrm{tr}(\phi) + \mathrm{tr}(\psi)$,

(ii) $\mathrm{tr}(\phi^2) = \mathrm{tr}(\phi)^2 - 2\deg(\phi)$,

(iii) $\phi^2 - [\mathrm{tr}(\phi)]\phi + [\deg(\phi)] = 0$

EXERCISE 9. Let $E/\mathbb{F}_q$ be an elliptic curve with p an odd prime. Show that there exists an elliptic curve $E'/\mathbb{F}_p$ with

$$\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2(p+1).$$

Show further that the groups $E(\mathbb{F}_p) \times E'(\mathbb{F}_p)$ and $E(\mathbb{F}_{p^2})$ have the same order, but need not be isomorphic.

EXERCISE 10. Let E be an elliptic curve over $\mathbb{F}_p$ with p a prime and $\#E(\mathbb{F}_p) = p+1-a$, and let $\phi : E \longrightarrow E$ be the p-power Frobenius, i.e. $\phi : (x,y) \mapsto (x^p, y^p)$. Let $\psi = [a] - \phi$.

(i) Show that $\phi \circ \psi = \psi \circ \phi = [p]$.

(ii) Show that if ψ is separable then $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$.

(iii) Show that if $p \geq 5$ and $E[p] = 0$ then $\#E(\mathbb{F}_p) = p+1$.

Proof:

(i) The map ψ is the difference of isogenies and is therefore itself an isogeny. In particular, this means that ψ is a rational map. Since the Frobenius endomorphism $F : x \mapsto x^p$ on $\overline{\mathbb{F}_p} \longrightarrow \overline{\mathbb{F}_p}$ is a field homomorphism, it commutes with addition and multiplication on the level of field elements, and therefore it commutes with rational functions $g \in \overline{\mathbb{F}_p}(E)$. This in turn implies that $\phi \circ \psi = \psi \circ \phi$, since the Frobenius endomophism commutes with the rational functions that locally present ψ.

Applying problem 6 part (iii) and recalling that $a = \mathrm{tr}(\phi)$, we have

$$[\mathrm{tr}(\phi)]\phi - \phi^2 - [\deg(\phi)] = ([a] - \phi) \circ \phi - [\deg(\phi)] = 0.$$

In class, we used the fact that $\deg(\phi) = p$, so the above equation reduces to $\psi \circ \phi = [p]$.

(ii) We have the following string of equalities:

$$\begin{aligned}\#E[p^r] &= \#\ker([p^r]) \\ &= \#\ker(\phi^r \circ \psi^r) \\ &= \#\ker(\psi^r) \\ &= \deg(\psi^r) = p^r.\end{aligned}$$

That $\#\ker(\phi^r \circ \psi^r) = \#\ker(\psi^r)$ follows from the fact that ϕ is injective. To see this, recall that the Frobenius map $x \mapsto x^p$ is injective as a map $\overline{\mathbb{F}_p} \longrightarrow \overline{\mathbb{F}_p}$ because *every* field homomorphism is injective. The map $(x,y) \mapsto (x^p, y^p)$ is therefore also injective.

Now that we know the cardinality of $E[p^r]$, we know that $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ since this is the only group of order p up to isomorphism. Inducting on r, we have that $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ or $E[p^r] \cong \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ since $E[p^r]$ must both contain $E[p^{r-1}] \cong \mathbb{Z}/p^{r-1}\mathbb{Z}$ as a subgroup and have cardinality p^r. The latter option is impossible since all of its elements have order at most $p-1$ and $E[p^{r-1}] \cong \mathbb{Z}/p^{r-1}\mathbb{Z}$ by the inductive hypothesis. It must then be the case that $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$.

(iii) Let $\omega = \frac{dx}{y}$,and note that it an invariant differential of E. We have that

$$\phi^*(\omega) = \frac{d(x^p)}{y^p} = \frac{px^{p-1}dx}{y^p} = 0,$$

and by Lemma 6.3 from lecture,

$$\psi^*\omega = ([a]-\phi)^*\omega = [a]^*\omega - \phi^*\omega = [a]^*\omega = a\cdot\omega$$

where the final equality follows from problem 3. We know that ψ is inseparable by part (ii) since $E[p]=0$, hence the induced map $\psi^* : \Omega_E \longrightarrow \Omega_E$ is zero by Lemma 6.4 from lecture. In particular, this means that $a\cdot\omega = 0$, and because $\omega \neq 0$ and Ω_E forms a $\mathbb{F}_p$-vector space, $a = 0$ in $\mathbb{F}_p$. Hasse's bound tells us that $a \leq 2\sqrt{p}$, so $a < p$ when $p \geq 5$ and therefore $a = 0$ in $\mathbb{Z}$. Since $\#E(\mathbb{F}_p) = p+1-a$, we conclude that $\#E(\mathbb{F}_p) = p+1$.

$\square$