EXERCISES FOR TUTORIAL 3

AURORE GUILLEVIC

Exercises

- 2.13 on Legendre form $y^2 = x(x-1)(x-\lambda)$
- 2.17 on automorphisms of curves
- 2.19 on endomorphisms being well-defined
- 2.23 on twists of curves
- 2.18 on curves in characteristic 3
- 2.24 on curves in characteristic 2
- 3.1
- 3.2
- 3.4
- 3.5
- 3.7 points of order 3 are inflexion points
- 3.8

Exercise 1 (2.13)**.**

(a) Put the Legendre equation $y^2 = x(x-1)(x-\lambda)$ into Weierstrass form and use this to show that the j-invariant is

$$j = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} .$$

(b) Show that if $j \neq 0, 1728$, then there are six distinct values of λ giving this j, and that if λ is one such value then the full set is

$$\left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\right\}.$$

(c) Show that if $j = 1728$ then $\lambda \in \{-1, 2, 1/2\}$, and if $j = 0$ then $\lambda^2 - \lambda + 1 = 0$.

Solution 1.

(a) The Legendre form is $y^2 = x(x-1)(x-\lambda)$, $\lambda \neq 0, 1$. We develop the x-term to get a short Weierstrass form.

$$y^2 \quad = \quad x(x-1)(x-\lambda) = (x^2-x)(x-\lambda) = x^3 - x^2 - \lambda x^2 + x\lambda = x^3 - (1+\lambda)x^2 + \lambda x$$

A simple solution would be to use the formula of j-invariant of this form: $y^2 = x^3 + a_2x^2 + a_4x$, which is

$$j = 256\frac{(3a_4 - a_2^2)^3}{a_4^2(4a_4 - a_2^2)} ,$$

with $a_2 = -(1+\lambda)$ and $a_4 = \lambda$, one obtains $(4a_4 - a_2^2) = 4\lambda - (1 + 2\lambda + \lambda^2) = -(\lambda^2 - 2\lambda + 1) = -(\lambda-1)^2$, $(3a_4 - a_2^2) = 3\lambda - (1 + 2\lambda + \lambda^2) = -(\lambda^2 - \lambda + 1)$, and

$$j = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} .$$

In SageMath one obtains

```
QQl.<l> = QQ[]
E = EllipticCurve(QQl, [0,-(1+l),0,l,0])
E.j_invariant().factor()
(256) * (l - 1)^-2 * l^-2 * (l^2 - l + 1)^3
```

With the short Weierstrass form: To cancel the x^2 term in a cubic $f(x) = x^3 + a_2x^2 + a_ax + a_6$, one need the change of variables $x \mapsto t = x + a_2/3$. Then $f(x) = f(t - a_2/3) = t^3 + (a_4 - a_2^2/3)t + 2/27a_2^3 - a_2a_4/3 + a_6$. With $a_2 = -1 - \lambda$, $a_4 = \lambda$ and $a_6 = 0$,

$$\begin{aligned} y^2 &= t^3 + (\lambda - (1+\lambda)^2/3)t - 2/27(1+\lambda)^3 + (1+\lambda)\lambda/3 \\ &= t^3 - (\lambda^2 - \lambda + 1)/3t - (1+\lambda)/27(\lambda^2 - 5\lambda + 2) \\ &= t^3 - (\lambda^2 - \lambda + 1)/3t - (1+\lambda)(\lambda-1)(2\lambda-1)/27 \end{aligned}$$

Finally, the j-invariant is $j = 1728(4a^3)/(4a^3 + 27b^2)$ and we obtain the expected result.

Date: Week 3.

```
QQl.<l> = QQ[]
QQx.<x> = QQl[]
f = x*(x-1)*(x-l)
f(x+(l+1)/3)
b, a = (f(x+(l+1)/3)).coefficients(sparse=False)[0:2]
print("f = {}\na = {} = {}\nb = {} = {}".format(f, a, a.factor(), b, b.factor()))
j = 1728*(4*a^3)/(4*a^3 + 27*b^2)
print("j = {}\n  = {}".format(j, j.factor()))
assert j == 2^8 *  (l^2 - l + 1)^3/((l - 1) * l)^2
```

and SageMath answer is

```
x^3 + (-1/3*l^2 + 1/3*l - 1/3)*x - 2/27*l^3 + 1/9*l^2 + 1/9*l - 2/27
f = x^3 + (-l - 1)*x^2 + l*x
a = -1/3*l^2 + 1/3*l - 1/3 = (-1/3) * (l^2 - l + 1)
b = -2/27*l^3 + 1/9*l^2 + 1/9*l - 2/27 = (-2/27) * (l - 2) * (l - 1/2) * (l + 1)
j = (256*l^6 - 768*l^5 + 1536*l^4 - 1792*l^3 + 1536*l^2 - 768*l + 256)/(l^4 -2*l^3 + l^2)
  = (256) * (l - 1)^-2 * l^-2 * (l^2 - l + 1)^3
```

(b) $j \neq 0, 1728$. From the expression of the j-invariant in terms of λ, one expresses the parameter λ in terms of j. This is

$$j = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} \iff j\lambda^2(\lambda-1)^2 = 256(\lambda^2-\lambda+1)^3 \text{ where } j \neq 0$$
$$\iff 256\lambda^6 - 768\lambda^5 + (1536-j)\lambda^4 + (2j-1792)\lambda^3 + (1536-j)\lambda^2 - 768\lambda + 256 = 0$$

To check if this sextic polynomial $S_j(\lambda)$ has simple roots, one compute its derivative then the resultant $\text{Resultant}(S_j(\lambda), S_j'(\lambda))$, with SageMath one obtains

$$\text{Resultant}(S_j(\lambda), S_j'(\lambda)) = 2^{38}j^4(j-1728)^3$$

hence it has only simple roots when the resultant is non-zero, that is, when $j \neq 0, 1728$. In this case, because it has degree 6, it has six distinct roots. One can check with SageMath that replacing λ by the five other values, we obtain a multiple of S_j. Alternatively, one can check that $j(\lambda) = j(\sigma(\lambda))$ with $\sigma(\lambda)$ in the set of the six values.

```
QQj.<j> = QQ[]
QQl.<l> = QQj[]
J = 2^8 *  (l^2 - l + 1)^3/((l - 1) * l)^2
Sj = J.numerator() - J.denominator()*j
Sj == 256*(l^2-l+1)^3 - l^2*(l-1)^2 * j
print("Sj = {}\n   = {}".format(Sj, Sj.factor()))
print("resultant = {}".format(Sj.resultant(Sj.derivative()).factor()))
for L in [l, 1-l, 1/l, 1/(1-l), l/(l-1), (l-1)/l]:
    assert J(L) == J
```

(c) $j = 1728$: we solve

$$1728 = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} \iff 3^3\lambda^2(\lambda-1)^2 = 4(\lambda^2-\lambda+1)^3 \iff 4\lambda^6-12\lambda^5-3\lambda^4+26\lambda^3-3\lambda^2-12\lambda+4 = 0$$

and the factorization is

$$(\lambda-2)^2(\lambda+1)^2(2\lambda-1)^2$$

we can see that there are three distinct roots $\{2, -1, 1/2\}$ where they each have multiplicity 2.

For $j = 0$, we solve the numerator to be zero:

$$j = 0 \iff (\lambda^2-\lambda+1)^3 = 0 \iff \lambda = \frac{1+\sqrt{-3}}{2}$$

the roots are the two primitive sixth roots of unity, each with multiplicity three.

```
Sja = J.numerator() - J.denominator()*1728
Sja.factor()
Sjb = J.numerator()
Sjb.factor()
(64) * (l - 2)^2 * (l + 1)^2 * (2*l - 1)^2
(256) * (l^2 - l + 1)^3
```

Exercise 2 (2.17)**.**

(a) Show that $(x, y) \mapsto (x, -y)$ is a group homomorphism from E to itself, for any elliptic curve in Weierstrass form.

(b) Show that $(x, y) \mapsto (\zeta x, -y)$ where ζ is a nontrivial cube root of unity, is an automorphism of the elliptic curve $y^2 = x^3 + B$.

(c) Show that $(x, y) \mapsto (-x, iy)$ where $i^2 = -1$, is an automorphism of the elliptic curve $y^2 = x^3 + Ax$.

Solution 2. Let $E\colon y^2 = x^3 + Ax + B$ in short Weierstrass form. In each case, we need to show for an application ϕ and two points $P, Q \in E$ that (1) $\phi(P) \in E$, and (2) $\phi(P) + \phi(Q) = \phi(P + Q)$, $\phi([2]P) = [2]\phi(P)$. We denote $P(x_1, y_1)$, $Q(x_2, y_2)$, $\lambda = (y_2 - y_1)/(x_2 - x_1)$ when $P \neq \pm Q$ and $\lambda = (3x_1^2 + A)/(2y_1)$ when $P = Q$, $y_1 \neq 0$. Then $P + Q = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$ and $[2]P = (x_4, y_4) = (\lambda^2 - 2x_1, \lambda(x_1 - x_4) - y_1)$.

(a) $\phi\colon (x, y) \mapsto (x, -y)$ is the negation map in characteristic not 2.

First, $\phi(x, -y) \in E$ because $y^2 = (-y)^2$. Second, we will show that $-P - Q = -(P + Q)$ and $-[2]P = [2](-P)$. From the addition law in short Weierstrass form, $\lambda_{P,Q} = (y_2 - y_1)/(x_2 - x_1)$, $\lambda_{-P,-Q} = (-y_2+y_1)/(x_2-x_1) = -\lambda_{P,Q}$, and $x_3 = \lambda_{P,Q}^2 - x_1 - x_2$, hence $x_3' = (-\lambda_{P,Q})^2 - x_1 - x_2 = x_3$. For the y-coordinate, $y_3 = \lambda_{P,Q} \cdot (x_1 - x_3) - y_1$, and we deduce $y_3' = -\lambda_{P,Q} \cdot (x_1 - x_3) + y_1 = -y_3$, so that $(-P - Q) = -(P + Q)$. For doubling, the formula is the same but with $\lambda(P, P) = (3x_1^2 + A)/(2y_1)$, hence $\lambda(-P, -P) = -\lambda(P, P)$ and the rest is the same, so that $[-2]P = [2](-P)$.

(b) $\phi\colon (x, y) \mapsto (\zeta x, -y)$ is an automorphism on a curve of j-invariant 0 ($A = 0$). First, $\phi(x, y) \in E$ because $\zeta^3 = 1$.

Then we compute $(\zeta x_1, y_1) + (\zeta x_2, y_2) = (x_3', y_3')$ for two points $P(x_1, y_1)$ and $Q(x_2, y_2)$. We have $\lambda_\phi = (y_2 - y_1)/(\zeta(x_2 - x_1)) = \lambda/\zeta$. Then $x_3' = \lambda_\phi^2 - \zeta x_1 - \zeta x_2 = \lambda^2/\zeta^2 - \zeta(x_1 + x_2) = \zeta\lambda^2 - \zeta(x_1 + x_2) = \zeta x_3$ with $\zeta^3 = 1$ and $x_3 = \lambda^2 - x_1 - x_2$. Then, $y_3' = \lambda_\phi(\zeta x_1 - x_3') - y_1 = \lambda/\zeta(\zeta x_1 - \zeta x_3) - y_1$ and the ζ simplify to get $y_3' = \lambda(x_1 - x_3) - y_1 = y_3$. We obtain $\phi(P) + \phi(Q) = (x_3', y_3') = (\zeta x_3, y_3) = \phi(P + Q)$.

For the doubling, $\lambda_\phi = (3\zeta^2 x_1^2)/(2y_1) = \zeta^2\lambda$. Similarly, $x_4' = \lambda_\phi^2 - 2x_1\zeta = \zeta\lambda^2 - 2x_1\zeta = \zeta x_4$ where $x_4 = \lambda^2 - 2x_1$. For the y-coordinate, $y_4' = \lambda_\phi(\zeta x_1 - x_4') - y_1 = \zeta^2\lambda(\zeta x_1 - \zeta x_4) - y_1 = \lambda(x_1 - x_4) - y_1 = y_4$ and we conclude $(x_4', y_4') = (\zeta x_4, y_4)$ hence $[2]\phi(P) = \phi([2]P)$.

(c) $\phi\colon (x, y) \mapsto (-x, iy)$ is an automorphism on a curve of j-invariant 1728 ($B = 0$).

First, $\phi(x, y) \in E$ because $(iy)^2 = -y^2 = -x^3 - Ax = (-x)^3 + A(-x)$.

Then we compute $(-x_1, iy_1) + (-x_2, iy_2) = (x_3', y_3')$ for two points $P(x_1, y_1)$ and $Q(x_2, y_2)$. We have $\lambda_\phi = (iy_2 - iy_1)/(-x_2 + x_1)) = -i\lambda$. Then $x_3' = \lambda_\phi^2 + x_1 + x_2 = -\lambda^2 + x_1 + x_2 = -x_3$ with $i^2 = -1$ and $x_3 = \lambda^2 - x_1 - x_2$. Then, $y_3' = \lambda_\phi(-x_1 - x_3') - iy_1 = -i\lambda(-x_1 + x_3) - iy_1 = i\lambda(x_1 - x_3) - iy_1 = iy_3$. We obtain $\phi(P) + \phi(Q) = (x_3', y_3') = (-x_3, iy_3) = \phi(P + Q)$.

For the doubling, $\lambda_\phi = (3(-x_1)^2)/(2iy_1) = \lambda/i$. Similarly, $x_4' = \lambda_\phi^2 - 2(-x_1) = -\lambda^2 + 2x_1 = -x_4$ where $x_4 = \lambda^2 - 2x_1$. For the y-coordinate, $y_4' = \lambda_\phi(-x_1 - x_4') - iy_1 = -i\lambda(-x_1 + x_4) - iy_1 = i\lambda(x_1 - x_4) - iy_1 = iy_4$ and we conclude $(x_4', y_4') = (-x_4, iy_4)$ hence $[2]\phi(P) = \phi([2]P)$.

Exercise 3 (2.19)**.** Let $\alpha(x, y) = (p(x)/q(x), y \cdot s(x)/t(x))$ be an endomorphism of the elliptic curve E given by $y^2 = x^3 + Ax + B$, where p, q, s, t are polynomials such that p and q have no common root and s and t have no common root.

(a) Using the fact that (x, y) and $\alpha(x, y)$ lie on E, show that

$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}$$

for some polynomial $u(x)$ such that q and u have no common root. (Hint: Show that a common root of u and q must also be a root of p.)

(b) Suppose $t(x_0) = 0$. Use the facts that $x^3 + Ax + B$ has no multiple roots and all roots of t^2 are multiple roots to show that $q(x_0) = 0$. This shows that if $q(x_0) \neq 0$ then $\alpha(x_0, y_0)$ is defined.

Solution 3.

(a)

$$\begin{aligned}\alpha(x, y) \in E &\iff y^2 \frac{s^2(x)}{t^2(x)} = \frac{p^3(x)}{q^3(x)} + A\frac{p(x)}{q(x)} + B \\ &\iff (x^3 + Ax + B)\frac{s^2(x)}{t^2(x)} = \frac{p^3(x) + Ap(x)q^2(x) + Bq^3(x)}{q^3(x)}\end{aligned}$$

and one reads $u(x) = p^3(x) + Ap(x)q^2(x) + Bq^3(x)$. Reduce $u(x)$ modulo $q(x)$: $u(x) \bmod q(x) = p^3(x)$ and because by assumption $p(x)$ and $q(x)$ have no common root, we deduce that $u(x) \bmod q(x)$ has no common root with $q(x)$, then $u(x)$ has no common root with $q(x)$. In other terms, let x_0 be a root of $q(x)$, then $u(x_0) = p(x_0)^3 + Ap(x_0)\underbrace{q^2(x_0)}_{=0} + B\underbrace{q^3(x_0)}_{=0} = p^3(x_0) \neq 0$ because x_0 cannot be a root of $p(x_0)$ if it is a root of $q(x_0)$. Hence $u(x)$ and $q(x)$ do not share any root.

(b) Consider a root x_0 of $t(x)$, that is, $t(x) = (x - x_0)\tilde{t}(x)$.

$$(x^3 + Ax + B)\frac{s^2(x)}{t^2(x)} = \frac{u(x)}{q^3(x)} \iff (x^3 + Ax + B)\frac{s^2(x)}{(x - x_0)^2\tilde{t}^2(x)} = \frac{u(x)}{q^3(x)}$$

We know that $s(x_0) \neq 0$. First, we assume that $x_0^3 + Ax_0 + B \neq 0$. Hence we must have x_0 to be a root of $q(x)$. Second, we assume that $x_0^3 + Ax_0 + B = 0$, but because the cubic polynomial $x^3 + Ax + B$ has simple roots only, it writes $(x - x_0)(x^2 + ax + b)$ where the quadratic polynomial is not zero at x_0, we obtain

$$(x^2 + ax + b)\frac{s^2(x)}{(x - x_0)\tilde{t}^2(x)} = \frac{u(x)}{q^3(x)}$$

where $s(x_0) \neq 0$, so we conclude that $q(x_0) = 0$.

Exercise 4 (2.23)**.** Let E be given by $y^2 = x^3 + Ax + B$ over a field K and let $d \in K^\times$. The *twist* of E by d is the elliptic curve $E^{(d)}$ given by $y^2 = x^3 + Ad^2x + Bd^3$.

(a) Show that $j(E^{(d)}) = j(E)$.
(b) Show that $E^{(d)}$ can be transformed into E over $K(\sqrt{d})$.
(c) Show that $E^{(d)}$ can be transformed over K to the form $dy_1^2 = x_1^3 + Ax_1 + B$.

Solution 4.

(a) $j(E^{(d)}) = 1728\dfrac{4(Ad^2)^3}{4(Ad^2)^3 + 27(Bd^3)^2} = 1728\dfrac{4A^3 \cdot d^6}{4A^3d^6 + 27B^2d^6} = 1728\dfrac{4A^3}{4A^3 + 27B^2} = j(E)$ because $d \neq 0$.

(b) Let $\sqrt{d}$ be a square root of d, either in $\mathbb{K}$ is d is a square in $\mathbb{K}$, or in a quadratic extension $\mathbb{K}(\sqrt{d})$. Then the equation of E multiplied by $d^3 = \sqrt{d}^6$ is

$$\begin{aligned} d^3y^2 = d^3x^3 + Ad^2 \cdot dx + Bd^3 &\iff (d\sqrt{d}y)^2 = (dx)^3 + Ad^2(dx) + Bd^3 \\ &\iff y'^2 = x'^3 + Ad^2x' + Bd^3 \colon E^{(d)} \end{aligned}$$

hence $(x, y) \mapsto (dx, d\sqrt{d}y) \in E^{(d)}$ is defined over $\mathbb{K}(\sqrt{d})$.

(c) Divide by d^3 the equation of $E^{(d)}$:

$$\begin{aligned} &E^{(d)} \colon y^2 = x^3 + Ad^2x + Bd^3 \\ \iff &\frac{dy^2}{d^4} = \left(\frac{x}{d}\right)^3 + A\frac{x}{d} + B \end{aligned}$$

and the map $(x, y) \mapsto (x/d, y/d^2)$ sends a point on $E^{(d)}$ to a point on the other form $dy^2 = x^3 + Ax + B$, and the map is defined over $\mathbb{K}$ as it does not involve any root of d.

Exercise 5 (2.18)**.** Let $\mathbb{K}$ have characteristic 3 and let E be defined by $y^2 = x^3 + a_2x^2 + a_4x + a_6$. The j-invariant in this case is defined to be

$$j = \frac{a_2^6}{a_2^2a_4^2 - a_2^3a_6 - a_4^3}$$

(this formula is false if the characteristic is not 3).

```
F3 = GF(3)
F3a.<a2,a4,a6> = F3[]
E = EllipticCurve(F3a, [0,a2,0,a4,a6])
E.j_invariant().factor()
```

(a) Show that either $a_2 \neq 0$ or $a_4 \neq 0$ (otherwise, the cubic has a triple root, which is not allowed).
(b) Show that if $a_2 \neq 0$, then the change of variables $x_1 = x - (a_4/a_2)$ yields an equation of the form $y_1^2 = x_1^3 + a_2'x_1^2 + a_6'$. This means that we may always assume that exactly one of a_2 and a_4 is 0.

(c) Show that if two elliptic curves $y^2 = x^3 + a_2x^2 + a_6$ and $y^2 = x^3 + a_2'x^2 + a_6'$ have the same j-invariant, then there exists $\mu \in \overline{\mathbb{K}}^\times$ such that $a_2' = \mu^2 a_2$ and $a_6' = \mu^6 a_6$.

(d) Show that if $y^2 = x^3 + a_4x + a_6$ and $y^2 = x^3 + a_4'x + a_6'$ are two elliptic curves (in characteristic 3), then there is a change of variables $y \mapsto ay$, $x \mapsto bx + c$, with $a, b \in \overline{\mathbb{K}}^\times$ and $c \in \overline{\mathbb{K}}$, that changes one equation into the other. Note that this is $a_4'x$, not $a_4'x^2$, in the second curve equation.

(e) Observe that if $a_2 = 0$ then $j = 0$ and if $a_4 = 0$ then $j = -a_2^3/a_6$. Show that every element of $\mathbb{K}$ appears as the j-invariant of a curve defined over $\mathbb{K}$.

(f) Show that if two curves have the same j-invariant then there is a change of variables over $\overline{\mathbb{K}}$ that changes one into the other.

Solution 5.

(a) Let's compute the derivative of $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Because $3 = 0$ in characteristic 3, $f'(x) = 3x^2 + 2a_2x + a_4 = 2a_2x + a_4 = -a_2x + a_4$. We require $f(x)$ and $f'(x)$ to have no common root. The root of $f'(x)$ is $x_0 = -a_4/(2a_2) = a_4/a_2$, assuming $a_2 \neq 0$. We need to ensure that $f(x_0) \neq 0$: $f(a_4/a_2) = \frac{a_4^3}{a_2^3} + a_2\frac{a_4^2}{a_2^2} + a_4\frac{a_4}{a_2} + a_6 = \frac{a_4^3}{a_2^3} + 2\frac{a_4^2}{a_2} + a_6 = \frac{a_4^3 - a_4^2a_2^2 + a_2^3a_6}{a_2^3}$. It is non-zero for $a_4^3 - a_4^2a_2^2 + a_2^3a_6 \neq 0$. If $a_4 = 0$, $a_6 \neq 0$ is required. If $a_6 = 0$, $a_4 \neq 0$ is required.

For the case $a_2 = 0$, the derivative is $f'(x) = a_4$ and $a_4 \neq 0$ is required to avoid $f'(x)$ to be identically zero.

To conclude, if $a_2 \neq 0$ then one of a_4, a_6 should be non-zero, and if $a_2 = 0$, then a_4 should be non-zero. Finally, a_2 and a_4 cannot be zero simultaneously.

```
# (a)
F3ax.<x> = F3a[]
f = x^3 + a2*x^2 + a4*x + a6
f.derivative()
# -a2*x + a4
x0 = a4/a2
f.derivative()(x0) == 0
# True
f(x0)
# (-a2^2*a4^2 + a2^3*a6 + a4^3)/a2^3
F3a(f(x0).numerator())(a4=0)
# a2^3*a6
F3a(f(x0).numerator())(a6=0)
# -a2^2*a4^2 + a4^3
F3a(f(x0).numerator())(a4=0,a6=0)
# 0
```

(b) $x_1 = x - (a_4/a_2) \iff x = x_1 + a_4/a_2$, and $f(x) = f(x_1 + a_4/a_2) = (x_1 + a_4/a_2)^3 + a_2(x_1 + a_4/a_2)^2 + a_4(x_1 + a_4/a_2) + a_6$. Remember that $(x+a)^3 = x^3 + 3ax^2 + 3a^2x + a^3 = x^3 + a^3 \bmod 3$ and that $2 = -1 \bmod 3$. Hence $f(x) = x_1^3 + a_4^3/a_2^3 + a_2(x_1^2 + a_4^2/a_2^2 - x_1a_4/a_2) + a_4x_1 + a_4^2/a_2 + a_6 = x_1^3 + a_2x_1^2 + 2a_4^2/a_2 + a_4^3/a_2^3 + a_6 = x^3 + a_2'x^2 + a_6'$ with $a_2' = a_2$ and $a_6' = a_4^2/a_2(a_4/a_2^2 - 1) + a_6$.

(c) The generic formula of an isomorphism (that is which preserve the j-invariant) is $(x, y) \mapsto (x/\mu^2, y/\mu^3)$ from a curve $E\colon y^2 = x^3 + a_2x^2 + a_4x + a_6$ to another curve E'. The equation of the new curve is

$$(y/\mu^3)^2 = (x/\mu^2)^3 + a_2(x/\mu^2)^2 + a_4(x/\mu^2) + a_6 = x^3/\mu^6 + a_2x^2/\mu^4 + a_4x/\mu^2 + a_6 \ .$$

Because $\mu \neq 0$, one can multiply the equation by μ^6 to get

$$y^2 = x^3 + a_2\mu^2x^2 + a_4\mu^4x + a_6\mu^6 \ .$$

The new equation has $a_2' = a_2\mu^2$, $a_4' = a_4\mu^4$ and $a_6' = a_6\mu^6$. Here $a_4 = 0$, hence $a_2' = a_2\mu^2$ and $a_6' = a_6\mu^6$.

Alternatively, one can start from $j = j' \iff a_2^6/(-a_2^3a_6) = a_2'^6/(-a_2'^3a_6') \iff a_2^3/a_6 = a_2'^3/a_6' \iff \frac{a_2^3}{a_2'^3} = \frac{a_6}{a_6'}$. Denote the ratio $a_2/a_2' = \nu \in \mathbb{K}$, $a_6/a_6' = \nu^3$. In other terms, $a_2' = a_2/\nu$ and $a_6' = a_6/\nu$. With $\mu = 1/\sqrt{\nu}$ in $\mathbb{K}$ or a quadratic extension of $\mathbb{K}$, one gets the expected formulas $a_2' = a_2\mu^2$ and $a_6' = a_6\mu^6$.

(d) First, we note that the two curves have j-invariant 0 as $a_2 = a_2' = 0$.

Let's start from $f(x) = x^3 + a_4x + a_6$, with $x' = bx + c$ then $x = (x' - c)/b$ and compute $f(x) = f((x' - c)/b)$ for some non-zero b. $b^3f((x' - c)/b) = (x' - c)^3 + a_4b^2(x' - c) + b^3a_6 =$

$x'^3 - c^3 + a_4b^2x' - ca_4b^2 + b^3a_6 = x'^3 + a_4b^2x' + b^3a_6 - ca_4b^2 - c^3$ together with $y' = ay \iff y = y'/a$, we obtain that $y^2 = x^3 + a_4x + a_6$ corresponds to

$$E' \colon \frac{y'^2}{a^2} = f((x'-c)/b) = \frac{1}{b^3}\left(x'^3 + a_4b^2x' + b^3a_6 - ca_4b^2 - c^3\right)$$

One reads $a'_4 = a_4b^2 \iff b^2 = a'_4/a_4$ (where $a_4, a'_4 \neq 0$), then $b = \sqrt{a'_4/a_4}$ in $\mathbb{K}$ or in a quadratic extension of $\mathbb{K}$. Then we solve for c from the equation $a'_6 = b^3a_6 - ca_4b^2 - c^3$ that we rewrite, dividing by $b^3 \neq 0$:

$$\frac{a'_6}{b^3} = \left(\frac{-c}{b}\right)^3 + a_4\left(\frac{-c}{b}\right) + a_6$$

it also means that c is such that $(-c/b, \sqrt{a'_6/b^3})$ is a point on $E(\overline{\mathbb{K}})$.

From $a^2 = b^3$ we can set for example $a = \mu^3$ and $b = \mu^2$ for some non-zero μ, then $a^2 = \mu^6 = b^3$, and $a'_4 = \mu^4a_4$ and c should satisfy $a'_6 = \mu^6a_6 - ca_4\mu^4 - c^3$.

```
# (d) one need to add three variables a,b,c
F3 = GF(3) # define the field of 3 elements
F3a.<a2,a4,a6,a,b,c> = F3[] # a polynomial ring in characteristic 3
E = EllipticCurve(F3a, [0,a2,0,a4,a6])
F3ax.<x> = F3a[]
f = x^3 + a2*x^2 + a4*x + a6
f(a2=0)((x-c)/b)
b^3*f(a2=0)((x-c)/b)
# 1/b^3*x^3 + a4/b*x + (a6*b^3 - a4*b^2*c - c^3)/b^3
# x^3 + a4*b^2*x + a6*b^3 - a4*b^2*c - c^3
```

(e) For that we would like to obtain a formula like (2.9) page 47: in characteristic not 2 or 3, given a j-invariant not 0 or 1728, a curve equation in short Weierstrass form is $y^2 = x^3 + 3j(1728-j)x + 2j/(1728-j)$.

For $j = 0$, the curve equation has $a_2 = 0$. From 4, two curves E, E' with $a_2, a'_2 = 0$ are birationally equivalent[1] thanks to a change of variables, that is they are isomorphic and have the same j-invariant. We can choose $y^2 = x^3 + a_4x$ for some non-zero a_4.

For $j \neq 0$ and $a_4 = 0$, from $j = -a_2^3/a_6$ we deduce $a_6 = -a_2^3/j$, and a possible curve equation is $E \colon y^2 = x^3 + a_2x^2 - a_2^3/j$, for some non-zero a_2, for example $a_2 = j$ gives $y^2 = x^3 + jx^2 - j^2$.

(f) Combining the previous items gives the result: one needs to consider $j = 0$ and $j \neq 0$ separately.

One can read more about curves in characteristic 3 in Appendix A of Silverman's book "The Arithmetic of Elliptic Curves" at https://link.springer.com/book/10.1007/978-0-387-09494-6.

Proposition 1 ([Sil09, Prop. A.1.2 p.410])**.**

(a) *A curve given by a Weierstrass equation is nonsingular if and only if the discriminant of the equation is nonzero.*

(b) *Two elliptic curves E/K and E'/K are isomorphic over $\overline{K}$ if and only if they have the same j-invariant.*

(c) *Let E/K be an elliptic curve. Then $\mathrm{Aut}(E)$ is a finite group of order:*

2: *if $j(E) \neq 0, 1728$,*
4: *if $j(E) = 1728$ and $\mathrm{char}\, K \neq 2, 3$,*
6: *if $j(E) = 0$ and $\mathrm{char}\, K \neq 2, 3$,*
12: *if $j(E) = 0 = 1728$ and $\mathrm{char}\, K = 3$,*
24: *if $j(E) = 0 = 1728$ and $\mathrm{char}\, K = 2$.*

Proof of Prop. 1 for $\mathrm{char}\, K = 3$.

Case I: $\mathrm{char}\, K = 3$ and $j(E) \neq 0$. In this case E and E' have Weierstrass equations of the form

$$y^2 = x^3 + a_2x^2 + a_6 \ .$$

The only substitutions preserving this type of equation are

$$x = u^2x' \text{ and } y = u^3y' \ .$$

Since $j(E) = j(E')$, we have $a_2^3a'_6 = a'^3_2a_6 \neq 0$, so taking $u^2 = a_2/a'_2$ gives an isomorphism from E to E'. Further, if $E = E'$, then we must have $u^2 = 1$, so $\mathrm{Aut}(E) \simeq \{\pm 1\}$.

[1] https://en.wikipedia.org/wiki/Birational_geometry

Case II: $\operatorname{char} K = 3$ and $j(E) = 0$. In this case E and E' have Weierstrass equations of the form

$$y^2 = x^3 + a_4 x + a_6 \ .$$

The substitutions preserving this form look like

$$x = u^2 x' + r \text{ and } y = u^3 y' \ .$$

Note that we have $a_4, a_4' \neq 0$. An isomorphism from E to E' is obtained by choosing u and r to satisfy

$$u^4 = a_4/a_4' \text{ and } r^3 + a_4 r + a_6 - u^6 a_6' \ .$$

Further, if $E = E'$, then automorphisms of E have

$$u^4 = 1 \text{ and } r^3 + a_4 r + (1-u^2)a_6 = 0 \ .$$

Since $a_4 \neq 0$, there are exactly 12 such pairs (u, r) making up $\operatorname{Aut}(E)$.

□

Exercise 6 (2.24)**.** Let $\alpha, \beta \in \mathbb{Z}$ be such that $\gcd(\alpha, \beta) = 1$. Assume that $\alpha \equiv -1 \pmod 4$ and $\beta \equiv 0 \pmod{32}$. Let E be given by $y^2 = x(x-\alpha)(x-\beta)$.

(a) Let p be prime. Show that the cubic polynomial $x(x-\alpha)(x-\beta)$ cannot have a triple root mod p.

(b) Show that the substitution

$$x = 4x_1, \ y = 8y_1 + 4x_1$$

changes E into E_1, given by

$$E_1 \colon y_1^2 + x_1 y_1 = x_1^3 + \frac{-\beta - \alpha - 1}{4} x_1^2 + \frac{\alpha\beta}{16} x_1 \ .$$

(c) Show that the reduction mod 2 of the equation for E_1 is $y_1^2 + x_1 y_1 = x_1^3 + e x_1^2$ for some $e \in \mathbb{F}_2$. This curve is singular at $(0,0)$.

(d) Let γ be a constant and consider the line $y_1 = \gamma x_1$. Show that if $\gamma^2 + \gamma = e$, then the line intersects the curve in part 3 to order 3, and if $\gamma^2 + \gamma \neq e$ then this line intersects the curve to order 2.

(e) Show that there are two distinct values of $\gamma \in \overline{\mathbb{F}_2}$ such that $\gamma^2 + \gamma = 2$. This implies that there are two distinct tangent lines to the curve E_1 mod 2 at $(0,0)$, as in Exercise 2.20.

Solution 6.

(a) the roots of $x(x-\alpha)(x-\beta)$ are $\{0, \alpha, \beta\}$. We need one of α, β to be non-zero modulo p to avoid a triple root. Thanks to $\gcd(\alpha, \beta) = 1$, then one cannot have $p \mid \alpha$ and $p \mid \beta$ at the same time, in other terms, we cannot have $\alpha = \beta = 0 \bmod p$, so there is no triple root.

(b) $x = 4x_1$, $y = 8y_1 + 4x_1$ corresponds to a curve equation

$$\begin{aligned}
(8y_1 + 4x_1)^2 &= 4x_1(4x_1 - \alpha)(4x_1 - \beta) \\
2^6 y_1^2 + 2^6 x_1 y_1 + 2^4 x_1^2 &= 2^6 x_1 - 2^4 x_1^2 \beta - 2^4 x_1^2 \alpha + 4 x_1 \alpha\beta \\
2^6 y_1^2 + 2^6 x_1 y_1 &= 2^6 x_1 - 2^4 x_1^2 (\alpha + \beta + 1) + 4 x_1 \alpha\beta \\
y_1^2 + x_1 y_1 &= x_1 - x_1^2(\alpha + \beta + 1)/4 + x_1 \alpha\beta/16
\end{aligned}$$

```
QQa.<a,b> = QQ[]
QQx.<x1,y1> = QQa[]
x = 4*x1
y = 8*y1 + 4*x1
f = x*(x-a)*(x-b)
print("f(x=4*x1)/64 - 1/4*x1^2 = {}".format(f/64 - 1/4*x1^2))
print("y^2/64 - 1/4*x1^2 = {}".format(y^2/64 - 1/4*x1^2))
# f(x=4*x1)/64 - 1/4*x1^2 = x1^3 + (-1/4*a - 1/4*b - 1/4)*x1^2 + 1/16*a*b*x1
# y^2/64 - 1/4*x1^2 = x1*y1 + y1^2
```

(c) From E_1, we consider $\alpha \equiv -1 \pmod 4$, that is, there exists α_0 such that $\alpha = 4\alpha_0 - 1$ and $\beta \equiv 0 \pmod{32}$, that is, there exists β_0 such that $\beta = 32\beta_0$. We obtain $\alpha + \beta + 1 = 4\alpha_0 - 1 + 32\beta_0 + 1 = 4(\alpha_0 + 8\beta_0)$ and $\alpha\beta/16 = 2(4\alpha_0 - 1)\beta_0$.

$$E_1 \colon y_1^2 + x_1 y_1 = x_1^3 - (\alpha_0 + 8\beta_0) x_1^2 + 2(4\alpha_0 - 1)\beta_0 x_1$$

now that we get rid of the factors 2 at the denominators, we can reduce modulo 2 and get $E_1 \bmod 2$: $y_1^2 + x_1 y_1 = x_1^3 + \alpha_0 x_1^2$ and we obtain the desired result with $e = \alpha_0$.

```
E1x = f/64 - 1/4*x1^2
E1y = y^2/64 - 1/4*x1^2
E2x = sum([xi*E1x.monomial_coefficient(xi)(a=4*a-1,b=32*b) for xi in E1x.monomials()])
E2y = sum([xi*E1y.monomial_coefficient(xi)(a=4*a-1,b=32*b) for xi in E1y.monomials()])
# x1^3 + (-a - 8*b)*x1^2 + (8*a*b - 2*b)*x1
# x1*y1 + y1^2
```

(d) Let $\mathcal{L}_1 \colon y_1 = \gamma x_1$ for some constant γ. The intersection with E_1 mod 2 is

$$\begin{aligned} y_1^2 + x_1 y_1 &= x_1^3 + e x_1^2 \\ \iff \gamma^2 x_1^2 + x_1 \gamma x_1 &= x_1^3 + e x_1^2 \\ \iff 0 &= x_1^3 + (e - \gamma^2 - \gamma) x_1^2 \\ \iff 0 &= x_1^2 (x_1 + e - \gamma^2 - \gamma) \end{aligned}$$

The roots of this equation are $x_1 = 0$ with multiplicity 2 and $x_1 = \gamma^2 + \gamma - e$ with multiplicity one. If moreover $\gamma^2 + \gamma = e$ then $x_1 = 0$ has multiplicity 3. We conclude that $\mathcal{L}_1$ intersects E_1 mod 2 at $(0, 0)$ with multiplicity 3 if $e = \gamma^2 + \gamma$, and multiplicity 2 otherwise.

(e) We consider $\gamma^2 + \gamma - e = 0$ in $\overline{\mathbb{F}_2}$. The derivative is $2\gamma + 1 = 1 \bmod 2$ and is non-zero, hence the quadratic has only simple roots, on other words, the two roots are distinct.

References

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer New York, NY, 2 edition, 2009. https://link.springer.com/book/10.1007/978-0-387-09494-6.

E-mail address: aurore.guillevic@inria.fr