# Exercises

Christophe Ritzenthaler

June 4, 2018

## 1 Review of some properties of curves

*Exercise* 1.1. Show that the conic $C/\mathbb{Q} : x^2 + y^2 = 3$ has no rational points.

*Exercise* 1.2. Compute the projective closure of $V(y - z^2, x - z^3) \subset \mathbb{A}^3$ over $\mathbb{Q}$.

*Exercise* 1.3. Is $C/\mathbb{Q} : \{x^2 + y^2 + z^2 + t^2 = 0,\ x^3 + y^3 + z^3 + t^3 = 0\}$ singular? If not, what is its genus?

*Exercise* 1.4. Is the rational map $\phi : V((Y^3 - ZX^2 + ZY^2)) \subset \mathbb{P}^2(\bar{\mathbb{Q}}) \to \mathbb{P}^1$ defined by $(X : Y : Z) \mapsto (X^2 : Y^2)$ regular at $(0 : 0 : 1)$?

*Exercise* 1.5. What is the uniformizer of $C/\mathbb{Q} : X^4 + Y^2Z^2 + ZY^3 + X^2Y^2 + Z^4 = 0$ at $(0 : 1 : 0)$?

*Exercise* 1.6. Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ over $\mathbb{Q}$ defined by $(X : Y) \mapsto (X^3(X - Y)^2 : Y^5)$. What are its ramification points and index of ramifications?

*Exercise* 1.7. Using Riemann-Hurwitz theorem, compute the genus of $C/\mathbb{Q} : x^3 + y^3 + z^3 = 0$.

*Exercise* 1.8. Using Riemman-Roch theorem, prove that any genus 1 curve with a rational point $O$ can be written in the form

$$y^2z + a_1yxz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

## 2 Models of curves with few(er) parameters

*Exercise* 2.1. We will look at genus 1 curve over a field $k$ which have a $k$-rational point (this is always the case of algebraically closed fields and also over finite fields, thanks to Hasse-Weil bound).

We are therefore in the situation above and we can assume that

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

1. Show that if characteristic $k \neq 2, 3$ then we can assume that $C = E_{A,B} : y^2 = x^3 + Ax + B$.

2. there exists an isomorphism $\phi : E_{A,B} \to E_{A',B'}$ such that $\phi(O) = O'$ if and only if there exists $u \in k^*$ such that $A = u^4 A'$ and $B = u^6 B'$ (using the R.R. spaces $\mathcal{L}(2O)$ and $\mathcal{L}(3O)$ show that an isomorphism between two Weierstrass models is of the form $(x, y) \mapsto (u^2 x + r, u^3 y + su^2 x + t)$).

3. Conclude that over $\bar{k}$,

$$\begin{cases} E_{A,B} \simeq y^2 + xy = x^3 - \frac{36x}{j-1728} - \frac{1}{j-1728}, & \text{if } j := 1728\frac{4A^3}{4A^3+27B^2} \neq 0, 1728; \\ E_{A,B} \simeq y^2 = x^3 + 1, & \text{if } j = 0; \\ E_{A,B} \simeq y^2 = x^3 + x, & \text{if } j = 1728. \end{cases}$$

   (you may use MAGMA for that).

Conclusion: we see that geometrically, genus 1 curves are determined by a unique parameter $j$ up to isomorphism.

4. Let us assume that $j \neq 0, 1728$. Show that if $E_{A,B} \simeq E_{A',B'}$ then $u^2 \in k^*$.

5. Deduce that the set of $k$-isomorphism classes of $E_{A,B}$ with a given $j$-invariant different from $0, 1728$ is in bijection with $k^*/(k^*)^2$.

6. If $k = \mathbb{F}_q$ conclude that for such an $E_{A,B}$, there exists only another $E_{A',B'}$ no isomorphic to $E_{A,B}$ with the same $j$-invariant. It is called its *quadratic twist*. Find an equation of it.

When $j = 0$ (resp. $j = 1728$) one gets up to 4 (resp. 6) twists (for the general theory, see Chap.X.2 in (Silverman 86). The morality is that we can run over all curves over $\mathbb{F}_q$ in $2q + \varepsilon$ steps.

More generally, we would like to write curves with as few coefficients as possible (for instance if one has to span over all isomorphism classes). This can be imagined in two flavor: over $\bar{k}$ or directly over $k$? Note that over $k$, one will look at $\bar{k}$-isomorphism classes and then if one wants $k$-isomorphism classes, use the theory of twists as for the genus 1 case. We will see that the first question is already quite hard: what is the minimum number of parameters we can expect? One can show that the set of curves of genus $g > 1$ up to $\bar{k}$-isomorphisms is an irreducible quasi-projective variety of dimension $3g - 3$ called the *moduli space of curves* (of genus $g$) and denoted $\boldsymbol{M}_g$. What we have proved for $g = 1$ is that $\boldsymbol{M}_1 \simeq \mathbb{A}^1$ (actually it's

$\boldsymbol{M}_{1,1}$). Hence, for $g = 2$ (resp. $3, 4, 5$) we cannot expect to write our curves with less than 3 (resp. $6, 9, 12$) coefficients. The following exercises will try to reach these bounds. Note that we cannot hope this to be always possible. At least for $g \geq 24$, $\boldsymbol{M}_g$ is of general type, in particular it is not unirational and we cannot build such a family.

*Exercise* 2.2. Let $C_i : y_i^2 = f_i(x_i)$ be two hyperelliptic curves of genus $g \geq 2$ over a field $k$ of characteristic different from 2 which are isomorphic. We are going to show that an isomorphism between $C_1$ and $C_2$ is of the form

$$\phi : (x_1, y_1) \mapsto \left( \frac{ax_1 + b}{cx_1 + d}, \frac{ey_1}{(cx_1 + d)^{g+1}} \right)$$

with $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(k)$ and $e \in k^*$.

1. Let $\iota_i$ be the hyperelliptic involution of $C_i$ and $K_i$ their fixed subfield in $k(C_i)$. By the unicity of the $\iota_i$, show that $\phi^* K_2 = K_1$, i.e. that $\phi$ induces an automorphisms $\widetilde{\phi} : \mathbb{P}^1 \to \mathbb{P}^1$ between the $x_i$.

2. Conclude that $x_2 = (ax_1 + b)/(cx_1 + d)$ as above.

3. Show that one can write $y_2 = (P(x_1)y_1 + Q(x_1))/(R(x_1)y_1 + S(x_1))$.

4. After transforming $y_2^2 = f_2(x)$, using the facts that $F_2$ is square free, prove that $R = 0$, that $P$ is constant and then that $Q = 0$. Using the equality of the degrees of $f_i$ prove that $S = 0$ also.

Show that over $\bar{k}$, we can always write a genus 2 curve $C : y^2 = x(x - 1)P(x)$ where $P$ is a monic degree 3 polynomial. What is the smallest number of coefficients you can get over a finite field $k$?

*Exercise* 2.3. Let $C : F(x, y, z) = 0$ be a non-hyperelliptic curve of genus 3 over a field $k$, canonically embedded as a plane smooth quartic. We will assume that char $k \neq 2, 3$.

1. Prove that $C$ has a flex $P$ over $\bar{k}$ (actually this is the case in all characteristics as these points are Weierstrass points which always exist but for the rest of the exercise this assumption on the characteristic is anyway useful).

2. Transform $F$ by an element of $\mathrm{GL}_3(\bar{k})$ so that $P = (0 : 0 : 1)$ with tangent $x = 0$ to find an equation of the form

$$xz^3 + z \sum_{i=0}^{3} p_i x^{3-i} y^i + \sum_{i=0}^{4} q_j x^{4-j} y^j.$$

3. If $p_3 \neq 0$, show that you can moreover assume $p_3 = 1$, $p_2 = 0$ and $q_4 = 0$ or 1. Conclude on the number of parameters.

4. If $p_3 = 0$, show that you can assume $q_4 = 1$ and then $q_3 = 0$. Conclude.

In characteristic 2, a similar study is made in (Wall 95). In characteristic 3, we can also use another model, called the Riemann model to achieve 6 parameters. Over a finite field $\mathbb{F}_q$, the situation is more delicate. (Bergström 07) can obtain a family with 7 parameters when the curve has a rational point. Prove that this is the case if $q > 29$ (but there are pointless curves over $\mathbb{F}_{29}$).

*Exercise* 2.4. Let us end up with genus 5 curves. We will deal with the case where it is the complete intersection of three quadrics in $\mathbb{P}^4$ over an algebraically closed field $k$ of characteristic different from 2.

1. Let $Q_1, Q_2$ be two non-degenerate quadratic forms over $k$. Show that we can diagonalize $Q_1, Q_2$ in the same basis if $\det(Q_1 - xQ_2)$ has simple roots.

2. Use this result over $\bar{k}$ in the generic case to reduce the number of parameters to 15.

I do not know how to do less (=12). Here we have also an open entry in this web site: is there a genus 5 curve over $\mathbb{F}_7$ with 27 or 28 points?

## 3 Curves over finite fields

*Exercise* 3.1. Prove that a genus 0 or 1 curve over a finite field has always a rational point.

*Exercise* 3.2. Let $E/\mathbb{F}_3$ an elliptic curve with zeta function $Z(E/\mathbb{F}_3, T) = \frac{3T^2+2T+1}{(1-T)(3-T)}$. What is $\#E(\mathbb{F}_9)$?

*Exercise* 3.3. We want to prove Hasse-Weil-Serre bound: for any curve $C/\mathbb{F}_q$ of genus $g$, one has

$$\#C(\mathbb{F}_q) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

1. Show that if $\alpha_i$ is a root of the Weil polynomial then $\bar{\alpha_i}$ is too. One can therefore write

$$\#C(\mathbb{F}_q) = q + 1 - \sum_{i=1}^{g} \alpha_i + \bar{\alpha}_i.$$

2. Let $x_i = \lfloor 2\sqrt{q} \rfloor + 1 + \alpha_i + \bar{\alpha_i}$. Show that $x_i$ are totally positive algebraic integers. Conclude that $x_1 \cdots x_g \in \mathbb{Z}^{>0}$.

3. Use the arithmetic-geometric mean inequality to prove that $\sum_{i=1}^{g} x_i \geq g$.

4. Conclude. When is there equality?

*Exercise* 3.4. The previous bound can be improved in many direction. Let us study the constraints on curves with small *defect* $k$, *i.e.* $\mathbb{C}(\mathbb{F}_q) = q + 1 + g\lfloor 2\sqrt{q} \rfloor - k$.

1. Show from the previous exercise that if $k = 0$, then the numerator of the zeta function $f(T) = (qT^2 + mT + 1)^g$ where $m = \lfloor 2\sqrt{q} \rfloor$.

To go further, one needs the following result.

*Theorem* 3.5 (Siegel, M.A. vol. III, first paper). *If $\alpha$ is a totally positive algebraic integer of degree $d(\alpha)$ and $\alpha$ is not 1 or $\frac{3\pm\sqrt{5}}{2}$, then* $\mathrm{Tr}(\alpha) > \frac{3}{2}d(\alpha)$.

We are going to apply this result to the $x_i$ of the previous exercise.

2. Show that if $\mathrm{Tr}(\alpha) = d(\alpha) + k$ then apart from the two exceptional cases then $d(\alpha) < 2k$.

3. Show that if $k = 1$ then one can have only $\alpha = \frac{3\pm\sqrt{5}}{2}$ or 2.

Consider now the polynomial $P(T) = \prod_{i=1}^{g}(T - x_i)$. We write it as a product $P_1 \cdots P_t$ of irreducible polynomials which correspond to distinct Galois orbits of the $x_i$. We denote $\mathrm{Tr}(P_i)$ the opposite of the $\deg(P_i) - 1$ coefficient of $P_i$.

4. Show that $\sum_{i=1}^{g} x_i = g + k$.

5. Show that

$$\mathrm{Tr}(P) - \deg(P) = k = \sum_{i=1}^{t}(\mathrm{Tr}(P_i) - \deg(P_i))$$

where each summand is non-negative.

6. Conclude that if $k = 1$ then $P$ is of the form

$$(x-1)\cdots(x-1)\cdot(x-2) \qquad \text{or} \qquad (x-1)\cdots(x-1)\cdot(x^2-3x+1).$$

*Exercise* 3.6. Let $p$ be a prime and $q = p^2$. We denote by $C : X^{p+1} - Y^{p+1} - Z^{p+1} = 0 \subset \mathbb{P}^2$ a 1-dimensional projective algebraic set over $\mathbb{F}_q$.

1. Prove that $C$ is a curve and that its genus is $\frac{p^2-p}{2}$.
2. What upper bound do you get on $\#C(\mathbb{F}_q)$?

We want to show that $\#C(\mathbb{F}_q)$ reaches this upper bound. Recall that $\mathbb{F}_q^*$ is a cyclic group of order $p^2 - 1$ generated by a element $\zeta$.

3. Show that for $X^{p+1} = a$ with $a \in \mathbb{F}_q^*$ has a solution in $\mathbb{F}_q$ if $a^{p-1} = 1$. Prove that in that case the number of solutions is exactly $p + 1$.
4. Use this result to conclude on the number of $\mathbb{F}_q$-rational points on $C$.

Let us write the Weil polynomial of $C/\mathbb{F}_q$ as $f = \prod_{i=1}^{2g}(1 - \alpha_i T)$.

5. Prove that $\sum_{i=1}^{2g}(-\alpha_i) = \sum_{i=1}^{2g} |\alpha_i| = 2gp$.
6. Deduce from the first equality that $\alpha_i = -p$ and then a factorization of $f$ over $\mathbb{Q}$.