# Curves with many points

Jean-François Mestre
(written by Francesco Sica)

November 25, 1998

# Contents

# Introduction

The following notes have been written out of the course that professor Jean-François Mestre taught at McGill and Concordia universities as part of the Number Theory Seminar in april-may 1995.

Generally speaking, the course dealt with points on curves and related problems. The focus was drawn to rational points on elliptic curves or on jacobian of curves.

The first chapter consists of a certain number of tricks to find curves with as many points as possible.

Chapter two through six examine elliptic curves of high rank, reviewing the basics and exploring new results also under algebraic constraints (constant $j$-invariant) or via analytic methods (Weil's explicit formulas).

As an application of the previous chapters, chapter seven explains how to construct quadratic fields with large $p$-rank.

Chapters eight and nine study hyperelliptic curves (especially of genus 2), mostly from the elegant viewpoint of the theory of invariants.

These notes are essentially self contained provided you don't set off to cross examine every statement in them (in which case you might also find inaccuracies locally...). Since so much is yet to be done on the subject, the aim is for the most to give a taste of the methods used up to date and to leave the door open to new suggestions and improvements.

◊◊◊

Les notes qui suivent ont été rédigées à partir du cours que le professeur Jean-François Mestre donna à McGill et à Concordia en avril-mai 1995, dans le cadre du Séminaire de théorie des nombres du Québec et du Vermont.

L'objet du cours était principalement l'étude de courbes définies sur $\mathbf{Q}$ ayant beaucoup de points rationnels, et plus particulièrement l'obtention de courbes elliptiques de rang élevé.

Le premier chapitre présente plusieurs méthodes simples pour construire des courbes avec le plus possible de points rationnels.

Les chapitres deux à six étudient, après quelques rappels, les courbes elliptiques de rang élevé pour arriver à de nouveaux résultats en faisant aussi usage de méthodes analytiques (formules explicites de Weil). De nouveaux travaux concernant les courbes elliptiques de rang élevé et invariant constant y sont aussi présentés.

Les résultats des chapitres précédents s'appliquent pour construire des corps quadratiques ayant un $p$-rang élevé, ce qui est l'objet du chapitre sept.

Les chapitres huit et neuf sont consacrés aux courbes hyperelliptiques (surtout de genre 2), en grande partie par le biais de la théorie des invariants.

Ces notes de cours se suffisent à elles-mêmes si le lecteur fait acte de foi pour certaines affirmations. Il est possible cependant que des résultats inexacts s'y soient glissés ... En fait, vu que beaucoup reste à découvrir, l'objectif de ces notes est surtout de familiariser le lecteur avec les méthodes employées jusqu'à aujourd'hui et de lui laisser la voie libre pour aller plus loin.

Jean-François Mestre
Francesco Sica

# Chapter 1

# Curves with many points

The main goal of this course is to present a range of different topics related to curves and points on them defined over certain number fields. The scope of this chapter is to introduce a certain number of "tricks" to cope with conjectures giving information about the number of points on curves defined over a number field.

## 1.1 General problems and general statements

The starting point is Faltings' theorem (ex Mordell conjecture):

**Theorem 1 (Faltings, 1983)** *Let C be a curve of genus $g \geq 2$ over a number field K. Then C(K) the set of K-rational points of C is finite.*

¿From this theorem many questions arise:

1. **Effectivity**:
   - There is an effective bound on the number of points on $C(K)$ (Parshin).
   - There is no effective bound on the height of points of $C(K)$.
2. C/**Q** **fixed**: Suppose we are given a sequence of number fields $\ldots \subset K_n \subset K_{n+1} \subset \ldots$. How does $\#C(K_n)$ grow?
3. K, g **fixed**: Define

$$B(g, K) = \sup_{C/K \text{ of genus } g} \#C(K)$$

   Then

**Conjecture 1** *$B(g,K) < \infty$ if $g > 1$.*

It is not even known whether $B(2,\mathbf{Q}) < \infty$.

4. g **fixed**: It is trivially false that $sup_K B(g,K) < \infty$ . Nonetheless there is a conjecture:

   **Conjecture 2** *There exists a positive constant $N = N(g)$ such that for any number field $K$, there exist a finite number of $C/K$ of genus $g$ with $\#C(K) > N(g)$.*

A generalization of Faltings' theorem to higher dimensional varieties was formulated by Lang and Vojta:

**Conjecture 3 (Lang, Vojta)** *Let $K$ be a number field and $V/K$ a variety of "general type". Then*

*1) $V(K)$ is not Zariski dense in $V(\overline{K})$.*

*2) Moreover $\exists$ $W/K$, Zariski closed, $W \subset_{\neq} V$ such that for any number field $L \supset K$ we have $V(L) - W(L)$ is finite.*

We have the remarkable result connecting these conjectures to the previous ones:

**Theorem 2 (Caporaso, Harris, Mazur)** *Lang's first conjecture implies conjecture 1. Lang's second conjecture implies conjecture 2.*

We give an indication of the proof in the case we have a family of curves with one parameter.

Let $V = \{(x,y,t) \in \overline{\mathbf{Q}}^3 : f(x,y,t) = 0\}$ for a given $f \in \mathbf{Q}[x,y,t]$ be a surface of general type such that the fiber $V_t$ in $t$ is given by curves of genus at least 2. Lang-Vojta's first conjecture says that there exists a curve $C \subset V$ defined over $\mathbf{Q}$ such that $\#V(\mathbf{Q}) - \#C(\mathbf{Q}) < \infty$. This implies that $C$ is not vertical, i.e. is not contained in any $V_t$, otherwise $\#V(\mathbf{Q}) = \#\{V(\mathbf{Q}) - C(\mathbf{Q})\} + \#C(\mathbf{Q})$ would be finite, the first term of the sum being finite by the above, the second by Faltings' theorem. Thus $B(g,K)$ would be trivially finite for this family of curves.

We may therefore suppose that $C$ "depends" on $t$. Again by Faltings, $C(\mathbf{Q}) \bigcap V_t$ is finite. We then consider the map $\phi$:

$$\begin{array}{rcl} C & \longrightarrow & \overline{\mathbf{Q}} \\ (x,y,t) & \longmapsto & t \end{array}$$

Clearly $B(g,K)$ over this family of curves is then bounded by $\deg\phi + \#\{V(\mathbf{Q}) - C(\mathbf{Q})\}$.

□

## 1.2 How to obtain lower bounds on $B(g,K)$ and $N(g)$?

This section is by no way conventional. We will work through several examples to construct curves with many points. Let's begin with a general example:

1. **Plane curve of degree n**: Let $x^n + a_1x^{n-1}y + \cdots$ be the equation of a general curve of degree $n$. Then we have $(n+2)(n+1)/2$ parameters (coefficients) associated to such a curve. We can therefore construct a curve $C$ of degree $n$ which passes through $(n+2)(n+1)/2 - 1$ given points, and $C$ can be expected to be nonsingular if the points are in general position. Hence the genus of $C$ is $(n-1)(n-2)/2$ and we have produced a family of curves of genus $g$ with $g$ rational points approximately.

2. **Curves with many automorphisms**: Consider the curve $C$ given in affine coordinates by $\{(x,y) \in \mathbf{C}^2 : \ y^2 = f(x)\}$ where $f \in \mathbf{Q}[x]$ is separable of degree $2g+2$. This curve has $2g+4$ coefficients (one coming from $y$), therefore we can choose $2g+3$ general points which will lie on such a curve. Since $(x,y) \in C \Rightarrow (x,-y) \in C$ we obtain that $C$ has $4g+6$ rational points.

3. Let $P$, $Q$ and $R$ be polynomials in one variable of degree $\leq g+1$. Consider the curve $C$ given by the equation $y^2P + yQ + R = 0$. This curve is birationally equivalent to $Y^2 = Q^2 - 4PR$ which is a curve of genus $g$ in general. This time we can fix $3(g+2)-1$ points to lie on $C$. Since again we have an involution of $C$ we obtain a total of $6g+10$ rational points on $C$.

This suggests that maybe $B(g,K)/g < \infty$... At least we can say:

**Theorem 3** *1. We have the following lower bounds on $B(g,\mathbf{Q})$:*

- $B(g, \mathbf{Q}) \geq 8g + 16$
- $g \equiv 1 \pmod 4 \Rightarrow B(g, \mathbf{Q}) \geq 8g + 24$
- $g \equiv 3 \pmod 4 \Rightarrow B(g, \mathbf{Q}) \geq 8g + 40$
- $g \equiv 2 \pmod 3 \Rightarrow B(g, \mathbf{Q}) \geq 8g + 32$

*2.* $N(g) \geq 16(g+1)$

We will make wide use of the following lemma:

**Lemma 1** *Let $K$ be any field with char $K \neq 2$. Let $p \in K[x]$ be monic of degree $2n$. Then there exist two unique polynomials $q$ and $r$ in $K[x]$, $q$ monic, $\deg q = n$, $\deg r \leq n-1$, such that $p = q^2 - r$.*

Proof: In writing

$$p(x) = x^{2n} + a_{2n-1}x^{2n-1} + \cdots = (x^n + b_{n-1}x^{n-1} + \cdots)^2 - r(x)$$

we see that $a_{2n-i} = 2b_{n-i}+$ polynomial terms involving only $b_{n-j}$ for $j < i$, this holding for $i \leq n$. Therefore the result is clear.

□

Let's apply this lemma to the construction of our curves:

1. Writing the degree of polynomials as subscripts, we let, as in lemma 1:

$$p_{4g+4}(x) = \prod_{i=1}^{4g+4} (x - a_i) = q^2 - r_{2g+1}$$

where $a_i \in \mathbf{Q}$. Consider then the curve $C$ given by the equation $y^2 = r_{2g+1}(x)$. In general, $C$ will be of genus $g$ and we readily check that the points $(a_i, \pm q(a_i)) \in C(\mathbf{Q})$. $C$ has therefore (at least) $8g + 8$ rational points.

2. Now take

$$p_{2g+4}(x^2) = \prod_{i=1}^{2g+4} (x^2 - a_i^2) = q_{g+2}^2(x^2) - r_{g+1}(x^2)$$

and the curve $C$ given by $y^2 = r_{g+1}(x^2)$ of general genus $g$. Then the points $(\pm a_i, \pm r_{g+1}(a_i^2)) \in C(\mathbf{Q})$, showing $4(2g+4) = 8g + 16$ rational points on $C$, which is the lower bound for a general curve given in theorem 3.

We can now generalize this idea further: suppose we take an hyperelliptic curve $C$ given by $y^2 = f(x)$ where $f \in \mathbf{Q}[x]$. We are looking for curves which are stable under certain groups of automorphisms $G$ to obtain from $k$ points on the curve another $(k-1)\,|G|$ points. On $C$ we have a unique canonical involution $w$, given in our coordinates by $w(x,y) = (x,-y)$. Moreover, it is a well-known result that if $g : C \longrightarrow C$ is an automorphism of $C$, then $g \circ w = w \circ g$. By writing $g$ as $(x,y) \longmapsto (u(x,y), v(x,y))$, for $(u,v) \in \mathbf{Q}(x,y)^2$, we then see that $u(x,y) = u(x,-y)$, i.e. $u$ does not depend on $y$ and therefore $u \in \mathrm{Aut}(\mathbf{P}^1(\mathbf{Q}))$. Hence if $g \in \tilde{G} \subset \mathrm{Aut}(C)$, then $u \in \mathrm{Aut}(\mathbf{P}^1(\mathbf{Q}))$. Also, if we know $u$ we can recover $g$ modulo $w$.

We now want to characterize the possible finite $\tilde{G}$ that can occur. By the above we need examine only the finite subgroups $G \subset \mathbf{PGL}_2(\mathbf{Q})$.

Remark: $\alpha \in G \Rightarrow \mathrm{ord}\alpha \leq 6$. This results after examining the compatibility of Galois action on the two eigenvalues of $\alpha$. Indeed if $\alpha^n = \lambda\mathbf{Id}$ then $\sqrt[n]{|\lambda|}$ is quadratic over $\mathbf{Q}$ (or rational), hence the eigenvalues of $\alpha$ are $\sqrt[n]{|\lambda|}$ times a root of unity (at most 12-th root). Rule out the impossible cases to arrive to the the result.

By Klein's theorem and by the remark the only possible $G$'s are $1, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/6\mathbf{Z}, D_3, D_4, D_6$ and these indeed occur as we show in the table below (we also write the corresponding invariant function, i.e. a generator of $\mathbf{Q}(x)^G$).

| | | |
|---|---|---|
| $\mathbf{Z}/2\mathbf{Z}$ | $< x \mapsto -x >$ | $s_2 = x^2$ |
| $\mathbf{Z}/3\mathbf{Z}$ | $< x \mapsto \frac{1}{1-x} >$ | $s_3 = \dfrac{x^3 - 3x + 1}{x(x-1)}$ |
| $\mathbf{Z}/4\mathbf{Z}$ | $< x \mapsto \frac{x+1}{1-x} >$ | $s_4 = \dfrac{x^4 - 6x^2 + 1}{x(x-1)(x+1)}$ |
| $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ | $< x \mapsto \frac{1}{x}, x \mapsto -x >$ | $\tilde{s}_4 = \dfrac{x^4 + 1}{x^2}$ |
| $\mathbf{Z}/6\mathbf{Z}$ | $< x \mapsto \frac{3}{3-x} >$ | $\tilde{s}_6 = \dfrac{(x^3 - 6x^2 + 9x - 3)(x^3 - 9x + 9)}{x(x-1)(2x-3)(x-2)(x-3)}$ |
| $D_3$ | $< x \mapsto \frac{1}{1-x}, x \mapsto \frac{1}{x} >$ | $s_6 = \dfrac{x^2 - x + 1}{x^2(x-1)^2}$ |
| $D_4$ | $< x \mapsto \frac{x+1}{1-x}, x \mapsto -x >$ | $s_8 = s_4^2$ |

$$D_6 \quad < x \mapsto \tfrac{3}{3-x}, x \mapsto \tfrac{3}{x} > \quad s_{12} = \tilde{s}_6(x)\tilde{s}_6(\frac{3}{x})$$

Let's apply this characterization to our context:

1. Take $p_{2n}(x) = q^2(x) - r_{n-1}(x)$. Let $C$ be the curve given by $y^2 = r_{n-1}(s_8(x))$. Let $G \cong D_4$ be a group defined over $\mathbf{Q}$ associated to $s_8$. Pick $2n$ general values $x_1, \ldots, x_{2n}$ of $x$ to get $16n$ different values $(g \cdot x_i)$ $(g \in G)$. Note that $C$ is birationally equivalent to an hyperelliptic curve of degree $8(n-1)$ because $\deg s_8 = 8$. Therefore if we choose $g$ such that $2g + 2 = 8n - 8 \Leftrightarrow g = 4n - 5$ we get that the genus of $C$ is $g$. In taking
$$p_{2n}(x) = \prod_{i=1}^{2n} (x - s_8(x_i))$$
we get $2 \times 16n = 8g + 40$ rational points on $C$, which is the bound given in theorem 3 for $g \equiv 3 \pmod 4$.

2. Consider the group $C_n =< x \mapsto \zeta_n x >$, cyclic of order $n$. It is defined over $K = \mathbf{Q}(\zeta_n)$, and has $x^n$ as invariant function. Choose four different points $x_1^n, \ldots, x_4^n$ and let
$$p_4(x) = (x - x_1^n) \cdots (x - x_4^n) = q^2(x) - (\alpha x + \beta)$$
Take the curve $C$: $y^2 = \alpha x^n + \beta$, and suppose $n = 2g + 2$ so that $C$ has genus $g$. Then as before $C$ passes through the $8n = 16(g+1)$ points $(\zeta_n^j x_i, \pm q(x_i^n))$ $(1 \le i \le 4,\ 1 \le j \le n)$. Therefore there exist infinitely many curves defined over $K$ with at least $16(g+1)$ points over $K$, which is the lower bound for $N(g)$.

The bound for $N(g)$ in theorem 3 is the best one for $g > 6$ and $g \neq 9, 10, 45$. For small values of $g$, we have the following: long ago Brumer found $B(2, \mathbf{Q}) \geq 144$ and $B(3, \mathbf{Q}) \geq 72$. This was improved recently by Keller and Kulesz to $B(2, \mathbf{Q}) \geq 588$ and $B(3, \mathbf{Q}) \geq 176$ (cf [KK]). We refer to the paper of Elkies for an account of various methods to tackle these problems. In class we just mentioned the method of slicing surfaces. If $S$ is a smooth surface of $\mathbf{P}^3(\overline{\mathbf{Q}})$ of degree $d$ with $R$ lines then a generic plane slice of $S$ is a nonsingular curve of degree $d$ with at least $R$ points, thus making $N((d-1)(d-2)/2) \geq R$. We end by an example:

Example: Let $P \in \overline{\mathbf{Q}}[X, Y]$ be a homogeneous polynomial of degree $d$, and suppose that its zeros in $\mathbf{CP}^1$ are left invariant by a subgroup

$G \subset \mathbf{PGL}_2(\mathbf{C})$ of order $M$. Let $S$ be the surface $P(X,Y) = P(Z,T)$. Then, for any $(\alpha,\beta,\gamma,\delta) \in G$ we have:

$$P(\alpha X + \beta Y, \gamma X + \delta Y) = \lambda P(X,Y)$$

Since we have $d$ different determinations for $\lambda^{1/d}$, we get $Md$ lines on $S$ given by the general equation:

$$X = X, \quad Y = Y, \quad Z = \frac{\alpha X + \beta Y}{\lambda^{1/d}}, \quad T = \frac{\gamma X + \delta Y}{\lambda^{1/d}}$$

Also we have $d^2$ more lines

$$\{X - a_i Y = 0\} \bigcap \{Z - a_j T = 0\}$$

where the $a_k$ $(1 \leq k \leq d)$ are the roots of $P$. Hence $S$ contains at least $d(M+d)$ lines and it is a theorem that this is the exact number of lines on $S$. The problem of finding $P$ maximizing $M$ is explained in Elkies' paper [Elk] and is related to the existence of regular polyhedra inscribed in the Riemann sphere whose vertices are the zeros of $P$.

# Chapter 2

# Rank of elliptic curves

The purpose of chapters 2 and 3 is to construct families of elliptic curves of rank (at least) 8 and 11. Let's recall some general facts about cubics and elliptic curves.

## 2.1 General Facts

Let $C/K$ be a nonsingular cubic with a point $O \in C(K)$. Then we can endow $C(K)$ with an associative law $+$ to make it a commutative group in which $O$ is the identity. If $O$ is an inflexion point then the cubic is isomorphic to a plane cubic of the form

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

This is the Weierstraß model of the elliptic curve in which $O$ is the only point at infinity (therefore an inflexion point). In this case, for given points $P$ and $Q$ in $C(K)$, we can compute $P+Q$ by noticing that $P$, $Q$ and $-P-Q$ lie on the same line.

A cubic is determined by 9 points in general position (no three on the same line or six on the same conic). Therefore by 8 points in general position there passes a pencil of cubics $\alpha C_1 + \beta C_2$. Then there exists a ninth point which lies on all the cubics of the pencil (Tate produced a proof of the associativity of the addition law based on this fact).

**Theorem 4 (Mordell, Weil)** *Let $K$ be a number field or a function field, $E/K$ an elliptic curve. Then $E(K)$ is finitely generated i.e.*

$$E(K) \simeq \mathbf{Z}^r \times T$$

*where $T$ is a torsion group and $r$ is called the rank of $E/K$.*

We can ask ourselves if there is a way of finding an explicit system of generators. Regarding the torsion, we have the famous

**Theorem 5 (Mazur)** *If $K = \mathbf{Q}$ then $T$ is one of the following groups:*

$$\begin{array}{ll} \mathbf{Z}/n\mathbf{Z} & n = 1, \ldots, 10, 12 \\ \mathbf{Z}/2n\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} & n = 1. \ldots, 4 \end{array}$$

*and each of these can occur.*

Recently Merel [Mer] generalized this result:

**Theorem 6** *For any $d$ there exists a constant $M(d)$ such that for all $K$ with $[K : \mathbf{Q}] = d$ and all elliptic curves $E/K$ we have $|Tor\, E(K)| \leq M(d)$.*

Now we can ask ourselves:

- $K$ fixed: is $r$ bounded?
- Let $E/K$ be an elliptic curve and $K \subset K_1 \subset \ldots \subset K_n \subset \ldots$ a sequence of number fields. How does $\mathrm{rank}(E(K_n))$ grow with respect to $n$?

## 2.2 Independence of points on an elliptic curve

Consider the general problem: given $P_1, \ldots, P_s$ points in $E(K)$, how can we prove that they are linearly independent (over $\mathbf{Z}$)?

1. One method is to look at the reduction modulo 2, that is to observe that if the images of the $P_i$'s are independent in $E(K)/2E(K)$, then a fortiori they are independent in $E(K)$. A case by case verification involves $2^s$ computations, which makes the method unsuitable for large $s$.

2. Over number fields we have the notion of height $\hat{h}$ , that is a positive definite quadratic form defined over $E(K)/\mathrm{Tor}(E(K))$. Furthermore $\hat{h}$ is uniquely defined by the extra condition that for any $P$, $h(P) - \hat{h}(P) = O(1)$, where $h$ is the "naive" Weil height (Néron, Tate, cf [Silv] pages 277 and following). Then, after calling $< .,. >$ the bilinear pairing associated to $\hat{h}$ we have that the $P_i$'s are independent if and only if the matrix $(< P_i, P_j >)_{1 \leq i,j \leq s}$ is nonsingular.

How can we compute $\hat{h}(P)$?

Néron gives the formula (valid for $K = \mathbf{Q}$):

$$\hat{h}(P) = \sum \lambda_p(P) + \lambda_\infty(P)$$

where the sum runs over primes $p$ dividing the denominator of the abscissa $x(P)$ of $P$ and bad $p$'s. $\lambda_p(P)$ is equal to $\log p \times$ (a rational number with denominator dividing 12). The archimedean part is more complicated and involves trascendental numbers. Putting $z \in E(\mathbf{C})$ corresponding to $P$ we have:

$$\lambda_\infty(P) = -\log \sigma(z) + \mathrm{Re}(z\eta(z))/2$$

This formula is fast to converge but involves two transcendental functions. On the other hand, Tate gave in 1968 an alternative formula which is simpler but also slower:

$$\lambda_\infty(P) = -\frac{1}{2}\log|x(P)| + \frac{1}{8}\sum_n \frac{\log|Z(2^n P)|}{4^n}$$

where $Z$ is a certain rational function.

Remark: We see that in order to apply Néron's formula we have to compute $z$ with high precision. A good way to do this is by Landen's transform (1788) whose precision is quadratic (the precision is twice as good at each step, cf [BM]). Zagier gave an elegant but slower method. We give here a brief review of his method. Suppose for instance that $E$ is given in Legendre form $y^2 = f(x)$ and that $f$ has three real roots. Then its affine graph in $\mathbf{R}^2$ has two connected components. Call $E_1$ the "right" (unbounded) one. Also $E(\mathbf{C})$ can be viewed as a rectangle in $\mathbf{C}$ whose lower edge $(0, \omega_1)$ corresponds to $E_1$. Furthermore, the interval $(0, \omega_1/2)$ corresponds exactly to the "lower" part of $E_1$, i.e. to

$$E_2^1 = \{P \in E_1 : y(P) < 0\}$$

Therefore if $z$ corresponds to $P \in E_1$ then, writing $z/\omega_1$ in binary base:

$$P \in E_2^1 \iff \frac{z}{\omega_1} = 0.0\ldots$$

We can then proceed inductively by defining $P_n = 2^n P$. We can write:

$$\frac{z}{\omega_1} = \sum_{n\geq 1} \frac{\epsilon_n}{2^n}$$

where $\epsilon_n = 0 \Leftrightarrow P_{n-1} \in E_2^1$. Also recall that there is a quadratic algorithm to compute $\omega_1$ by the arithmetic-geometric mean (cf theorem 50).

We conclude this section by mentioning a theorem of Tate about heights:

**Theorem 7 (Tate)**

$$\hat{h}(P) = \lim_n \frac{h(2^n P)}{4^n}$$

## 2.3 Elliptic Curves of High Rank

Most of the cases where it is proven that there exist infinitely many curves of rank $r$ come by specialization in accordance with the following

**Theorem 8 (Néron 1952)** *Given an elliptic curve $E/\mathbf{Q}(t_1, \ldots, t_n)$ of rank $r$ and non constant $j$-invariant, there exist infinitely many $(t_1, \ldots, t_n) \in \mathbf{Q}^n$ such that the specialization of the curve has rank at least $r$.*

Proof: Call $K = \mathbf{Q}(t_1, \ldots, t_n)$. We will prove that there are points $P_1, \ldots, P_r$ in $E(K)$ such that their reductions modulo 2 are independent for infinitely many $(t_1, \ldots, t_n) \in \mathbf{Q}^n$. Note that since $E(K)$ is of rank $r$ we have that $[E(K)/2E(K)] \bigotimes_{\mathbf{F}_2} \mathbf{F}_2$ has dimension $r$ over $\mathbf{F}_2$ so that we can pick $P_1, \ldots, P_r$ independent in $E(K)/2E(K)$. Now to say that $P_1, \ldots, P_r$ are independent in $E(K)/2E(K)$ means that $2^r$ quadratic polynomials (with coefficients depending on $(t_1, \ldots, t_n)$) have no root in $K$, therefore they are irreducible over $K$. By Hilbert's irreducibility theorem for infinitely many specializations $(t_1, \ldots, t_n) \in \mathbf{Q}^n$ the polynomials obtained will remain irreducible over $\mathbf{Q}$, so that the specializations of the points $P_1, \ldots, P_r$ will be independent in $E(K)/2E(K)$ and a fortiori in $E(K)$.

□

Moreover Néron produced elliptic curves over $\mathbf{Q}(t)$ of rank at least 10 and, for any $g$, curves of genus $g$ (over $\mathbf{Q}(t)$) with Jacobian of rank at least $3g+6$, hence the following

**Theorem 9 (Néron)**

1. *There exist infinitely many elliptic curves of rank at least 10 over $\mathbf{Q}$ .*
2. *There exist infinitely many curves of genus $g$ such that their Jacobian has rank $r \geq 3g+6$.*

Similarly, working with curves defined over the function field of an elliptic curve of positive rank over the rationals, he finds

**Theorem 10 (Néron)** *1. There exist infinitely many elliptic curves of rank at least* 11 *over* $\mathbf{Q}$ .

*2. There exist infinitely many curves of genus $g$ such that their Jacobian has rank $r \geq 3g+7$.*

Silverman and Tate say more. Suppose we are given an elliptic surface $S$ with base $B$ $(= \mathbf{P}^1$ or an elliptic curve of rank at least one) defined over a field $k$. Then we can view $S$ as an elliptic curve over the global field $K = k(B)$. If we take a point $P \in E(K)$ we can consider its Néron-Tate height $\hat{h}(P)$. Also we can consider for nearly any fiber $E_b$ the Néron-Tate height of the specialisation $P_b$, namely $\hat{h}_k(P_b)$ . Finally we can speak also of the height $h(b)$ of elements of $B$. Call also $<.,.>$ and $<.,.>_k$ the first and second Néron-Tate height, respectively. We then have the following theorem:

**Theorem 11 (Silverman, Tate)** *We have the following equivalent facts:*

*1.*

$$\forall P \in E(K) \qquad lim_{\substack{b\in B(k) \\ h(b)\to+\infty}} \frac{\hat{h}_k(P_b)}{h(b)} = \hat{h}(P)$$

*2.*

$$\forall P,Q \in E(K) \qquad lim_{\substack{b\in B(k) \\ h(b)\to+\infty}} \frac{< P_b, Q_b >_k}{h(b)} =< P, Q >$$

**Corollary 1** • *For any $P \in E(K) - E(K)_{\rm tor}$ there exist finitely many $b \in B(k)$ such that $P_b$ is a torsion point.*

- *If $P_1, \ldots, P_n$ are independent sections of $S$, then there are finitely many $b \in B(k)$ such that their specializations are dependent.*

## 2.4 Néron's method as explained by Shioda

Shioda ([Shio 1]) describes in an elegant fashion Néron's method for constructing a family of elliptic curves defined over $\mathbf{Q}$ of rank (at least) 11.

Start with the curve $C_\infty$ defined over $\overline{\mathbf{Q}}$ by $y^2 = x^3$. Since $(0,0)$ is singular, this is not an elliptic curve. Nevertheless $C_\infty - (0,0)$ can be given an abelian group structure by defining a morphism:

$$\begin{array}{rcl} (\overline{\mathbf{Q}},+) & \longrightarrow & (C_\infty - (0,0),+) \\ u & \longmapsto & P(u) = (u^{-2}, u^{-3}) \end{array}$$

Also $P(u_1), P(u_2), P(u_3)$ are collinear if and only if $u_1 + u_2 + u_3 = 0$.

Define also $L(u)$ to be the line passing through $P(u)$ and tangent to $C_\infty - (0,0)$, i.e. passing through $P(-u/2)$. We can then verify that $L(u_1)$, $L(u_2)$, $L(u_3)$ are concurrent if and only if $u_1^{-1} + u_2^{-1} + u_3^{-1} = 0$.

Now take $u_i \in \mathbf{Q}$ $(1 \leq i \leq 8)$ such that

$$\sum_{i=1}^{8} u_i = 0$$

and

$$\frac{1}{u_1} + \frac{1}{u_2} + \frac{1}{u_3} = 0 \tag{2.1}$$

Consider the pencil of cubics passing through the eight points $P_0 = (\infty, \infty)$, $P_i = P(u_i)$ $(1 \leq i \leq 7)$. Then it is not difficult to see that the ninth base-point of the pencil is $P_8 = P(u_8)$. The pencil of cubics can also be seen as an elliptic surface $S$ over $\mathbf{Q}(t)$ (i.e. the base is $\mathbf{P}^1(\mathbf{Q})$). An element of the pencil can be written as

$$C_t = \{(x,y) \in \mathbf{Q}^2 : \sum_{i+j \leq 3} a_{ij} x^i y^j - t(y^2 - x^3) = 0\} \tag{2.2}$$

Suppose further that

$$\forall i,j,k \qquad\qquad u_i + u_j + u_k \neq 0$$

Then $S$ is an elliptic surface in the sense of [Shio 2], all the fibers are irreducible and except for a finite number of them, they are nonsingular (hence elliptic curves) (easy exercise). Moreover $P_1, \ldots, P_8$ are independent over $\mathbf{Q}(t)$, as we will see further in chapter 3.3.

**Construction of 3 more points**:

We have that

$$C_t \bigcap L(u_1) = \{P_1, M_1, M_1'\}$$

and the map $M_1 \mapsto t$ is ramified at $\infty$ by construction, therefore there exists one other ramified value of $t$, say $t_1 \in \mathbf{Q}$. The field $\mathbf{Q}(t)(M_1)$ is then a quadratic extension of $\mathbf{Q}(t)$ ramified at $\infty$ and $t_1$, therefore its discriminant is of the form $\Delta_1 = a_1(t - t_1)$ with $a_1 \in \mathbf{Q}$. Do the same with $u_2$ and $u_3$.

Then $M_i \in C_t$ (and therefore $M_i'$) is defined over $\mathbf{Q}$ if and only if $\Delta_i$ is a square. In general the new points $M_i$ are defined over $\mathbf{Q}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \sqrt{\Delta_3})$. Consider then the curve $B$ defined by

$$\begin{cases} y_1^2 & = \Delta_1 & = a_1(t - t_1) \\ y_2^2 & = \Delta_2 & = a_2(t - t_2) \\ y_3^2 & = \Delta_3 & = a_3(t - t_3) \end{cases}$$

Then $B$ is easily seen to be an intersection of two quadrics. Indeed after replacing $t$ in the second and third equations, we get

$$\begin{cases} y_2^2 & = & b_1 y_1^2 + b_2 \\ y_3^2 & = & b_3 y_1^2 + b_4 \end{cases}$$

After parametrizing the first equation (a cylinder) in $w$, we replace $y_1^2$ in the second equation to get an expression of the type $Y^2 = f(w)$ where $f$ is a polynomial of degree 4, i.e. $B$ is a curve of genus 1. If we can show that $B(\mathbf{Q}) \neq \emptyset$ then $B$ is an elliptic curve defined over $\mathbf{Q}$ and for any $Q = (y_1, y_2, y_3) \in B(\mathbf{Q})$ we have an elliptic curve $C_t/\mathbf{Q}$ over $Q$ with 11 rational points $P_1, \ldots, P_8, M_1, M_2, M_3$.

Claim: $B(\mathbf{Q}) \neq \emptyset$.

Indeed by assumption (2.1) $L(u_1), L(u_2)$ and $L(u_3)$ are concurrent in $R \in \mathbf{Q}^2$. Since $\{C_t\}$ is a pencil, we can choose $t_0 \in \mathbf{Q}$ such that $R \in C_{t_0}$. Since then $R \neq P_i$ and

$$\{R, P_i\} \subset L(u_i) \bigcap C_{t_0}$$

and all the points are rational we must have that $a_i(t_0 - t_i)$ is a square for $i = 1, 2, 3$, that is our claim.

Note that in general as soon as $B(\mathbf{Q}) \neq \emptyset$ there is more than one rational point on $B$ and it will be of infinite order (cf [Shio 1] for an example that is all we need), so that we can apply the theory of elliptic surfaces that follows up to prove the independence of the 11 points thus constructed.

# Chapter 3

# Elliptic Surfaces

We want now to prove the independence "in general" of the eleven points $P_1, \ldots, P_8, M_1, M_2, M_3$. We will do this through the theory of elliptic surfaces, as explained in [Shio 2].

Now we suppose the ground field $k$ is an algebraic closed field of arbitrary characteristic. Let $C$ be a smooth projective curve over $k$, to say $S$ is an elliptic surface over $C$ will always mean the following: $S$ is a smooth projective surface with a relatively minimal elliptic fibration

$$f: \; S \longrightarrow C$$

that is, $f$ is a surjective morphism such that

1. almost all fibres are elliptic curves and
2. no fibres contain an exceptional curve of the first kind (i.e. a smooth rational curve with self-intersection number -1).

Throughout the chapter, we assume that $f$ has a global section $O$ and that $f$ is not smooth, i.e. there is at least one singular fibre.

If we call $E$ the generic fibre if $f$ and $K = k(C)$, we then have that $E$ is an elliptic curve defined over the global field $K$ with a distinguished point $O$. We can therefore take $O$ as the identity of $E(K)$. Viceversa any $E/K$ we can substantially viewed as an elliptic surface by adding a finite number of singular fibres.

Example 1: In the notations of chapter 2 we see that the cubic $C_t$ is defined over $\overline{\mathbf{Q}}$ and that if $f(x, y, t) = 0$ is the equation of $C_t$, then by letting also $t$ vary we see that

$$\{(x, y, t) \in \overline{\mathbf{Q}}^3 : \; f(x, y, t) = 0\}$$

is the affine part of a smooth projective surface $S$ that is an elliptic surface over $\mathbf{P}^1$ (for example, the discriminant $\Delta$ of the generic fiber $E$ is a polynomial in $t$, therefore the only singular fibers correspond to the zeros of $\Delta$ and to $\infty$). Furthermore, the surface is rational because, except for the nine base points $P_0, \ldots, P_8$, given $x$ and $y$, you can recover $t$ such that $(x, y, t) \in S$ uniquely (just look at equation 2.2). In fancier terms, $S$ is the blow-up of $\mathbf{P}^2$ at the nine base points. The fibration is the trivial one: $(x, y, t) \to t$.

Let us return to the general context. The points in $E(K)$ correspond to global sections of $S$. From this viewpoint, we shall define a positive definite bilinear pairing on $E(K)/E(K)_{\text{tor}}$ by means of intersection theory of divisors on a surface.

We can also attach to a surface its arithmetic genus $\chi \in \mathbf{N}$ (Euler-Poincaré characteristic), which is shown to be positive in the case of an elliptic surface.

Example 2: Consider the case of $S$ over $\mathbf{P}^1$ given by $y^2 = x^3 + a(t)x + b(t)$ where $a, b \in \overline{\mathbf{Q}}(t)$ and suppose that $\infty$ is not a singular value. This implies that

$$\Delta = -4a(t)^3 - 27b(t)^2$$

and $\deg \Delta \equiv 0 \pmod{12}$ so that

$$\chi = \frac{\deg \Delta}{12}$$

Remark: We take for granted the fact that

**Lemma 2** *$S$ is rational if and only if $\chi = 1$.*

Finally, call

$$R = \{v \in C : \text{ the fiber } f^{-1}(v) \text{ is reducible}\}$$

Let us state now the main theorem of this chapter:

**Theorem 12 (Main Theorem)** *Let $S$ be an elliptic surface over $C$ of genus $g(C)$ as at the beginning. Then*

*1.*

$$rk\, E(K) \leq 12\chi - 4 + 2g(C)$$

2. *There exists a positive definite bilinear pairing (denoted by $< .,. >$) over $E(K)/E(K)_{\rm tor}$ such that*

$$< P, Q >= \chi + (O.P) + (O.Q) - (P.Q) - \sum_{v \in R} contr_v(P, Q)$$

*where $(P.Q)\ldots$ is the intersection number of the sections corresponding to $P$ and $Q$ on $S$, and $contr_v(P, Q)$ is a rational number with denominator $\leq 12$.*

Remarks:

1. The bilinear pairing in the theorem is essentially the Néron-Tate pairing seen in chapter 2.

2. $\mathrm{contr}_v(P, Q)$ depends on the intersection numbers of the components of the reducible fibres and uses a classification into Kodaira types (cf [Shio 2]).

3. Let us continue with our example related to Shioda's construction where we have a pencil of cubics. In this situation, $C = \mathbf{P}^1$ so that $g(C) = 0$, $\chi = 1$ and therefore $\mathrm{rk}E(\overline{\mathbf{Q}}(t)) \leq 8$. We cannot hope to go to 11 when $C = \mathbf{P}^1$, that's why the Néron-Shioda construction involves $C = B$ an elliptic curve of positive rank.

4. Note also that since a relation of linear dependence in $E(\overline{\mathbf{Q}}(t))$ gives a relation of algebraic dependence on the coefficients of the points, we have $\mathrm{rk}E(\overline{\mathbf{Q}}(t)) = \mathrm{rk}E(\mathbf{C}(t))$ by Hilbert's Nullstellensatz.

5. This implies in example 2 that if $\deg \Delta = 12$, then $\mathrm{rk}E(\mathbf{Q}(t)) \leq 8$.

**About intersection numbers**: Let $D$ and $D'$ be two algebraic curves on $S$. If they meet transversally (i.e. if the tangent spaces of $D$ and $D'$ are not the same at their common points), then $(D.D') = \#D \bigcap D'$ by definition.

Recall that two curves $D_1$ and $D_2$ are said to be algebraically equivalent if there exists an algebraic surface $\Gamma \subset \mathbf{C}^n$ and $t_1, t_2 \in \mathbf{C}$ such that

$$\Gamma_{t_i} = \{(x_1, \ldots, x_{n-1}, t_i) \in \Gamma\} = D_i$$

for $i = 1, 2$.

Then $(D.D')$ is defined in general up to algebraic equivalence and we can always find curves $\tilde{D} \sim D$ and $\tilde{D}' \sim D'$ such that $\tilde{D}$ and $\tilde{D}'$ meet transversally.

In conclusion the intersection number is defined on the Néron-Severi group $NS(S)$, which is defined as the group of divisors on $S$ modulo algebraic equivalence. Since in this case $NS(S)$ is a free group of finite rank $\rho$ it becomes with the intersection pairing an integral lattice.

**Theorem 13 (Hodge index theorem)** *The intersection pairing on $NS(S)$ is an indefinite bilinear form of signature $(1, \rho - 1)$.*

In our context if $P = (x(t), y(t))$ and $Q = (w(t), z(t))$, then $(P.Q)$ is equal to the number of solutions (counted with multiplicities) of

$$\begin{cases} x(t) & = & w(t) \\ y(t) & = & z(t) \end{cases}$$

If $P = Q$ then it is "known" that $(P.P) = -\chi$. Also, since by definition any two fibres of $S$ are algebraically equivalent we have that $(D.D) = 0$ if $D$ is contained in a fibre. This suggests the following terminology:

**Definition 1** *A vertical divisor is a divisor contained in a fiber. A horizontal divisor is a divisor which is not vertical.*

## 3.1 Idea of the proof of Main Theorem

Let $\mathcal{D}_{\text{ver}}$ be the image of the vertical divisors in $NS(S)$ and similarly for $\mathcal{D}_{\text{hor}}$. We then have

$$\mathcal{D}_{\text{hor}} + \mathcal{D}_{\text{ver}} = NS(S)$$

Now as in [Shio 2] we write, for a reducible fibre $F_v$:

$$F_v = f^{-1}(v) = \Theta_{v,0} \cup \bigcup_{i=1}^{m_v - 1} \Theta_{v,i}^{\mu_{v,i}}$$

where $\Theta_{v,i} \quad (0 \le i \le m_v - 1)$ are the irreducible components of $F_v$, $\mu_{v,i}$ their multiplicity, $m_v$ their number, such that $\Theta_{v,0}$ is the unique component of $F_v$ meeting the zero section (it appears with multiplicity one because of the minimality of the fibration).

If $D \in NS(S)$ we can write $D = D_{\text{hor}} + D_{\text{ver}}$ and if we view the generic fiber $E$ as a curve on $S$ the intersection product $D_{\text{hor}}.E$ is a well-defined K-rational 0-cycle whose degree is $(D_{\text{hor}}.E) = (D.E)$. We then define $D.E = D_{\text{hor}}.E$.

Shioda then shows that one can define a surjective homomorphism

$$\begin{array}{rccc} \psi : & NS(S) & \longrightarrow & E(K) \\ & D & \longmapsto & P \end{array}$$

where $P$ is defined via the Abel-Jacobi map so that

$$P - O \overset{\text{lin}}{\sim} D_{\text{hor}}.E - (D_{\text{hor}}.E)O$$

**Theorem 14 (Shioda)** *$\psi$ is surjective. Let $T = \ker \psi$. Then $T$ is free and generated by*

$$(O), \qquad F, \qquad \Theta_{v,i} \quad (1 \leq i \leq m_v - 1,\ v \in R)$$

*where $F$ stands for any fiber. Also $T = \mathcal{D}_{\text{ver}} + \mathbf{Z}(O)$ so that $\mathcal{D}_{\text{ver}}$ is free and*

$$rk(T) = 2 + \sum_{v \in R} (m_v - 1)$$

*If $\phi = \psi^{-1}$, then $\phi(P) = (P) \pmod T$ (to a point it associates the global section on $S$ modulo $T$).*

**Corollary 2** *We have*

$$rk(E(K)) \leq 12\chi - 4 + 2g(C) - \sum_{v \in R} (m_v - 1)$$

*to account for the first part of Main Theorem.*

Proof of corollary: By definition, we have that

$$12\chi = b_2 - 2b_1 + 2 = b_2 - 2g(C) + 2 \tag{3.1}$$

where $b_i$ is the $i$-th Betti number of $S$. Since $NS(S)$ injects into $\mathrm{H}^2(S, \mathbf{Z})$ we have that $\rho \leq b_2$ so that

$$\rho \leq 12\chi - 2 + 2g(C)$$

On the other hand, theorem 14 implies that

$$\mathrm{rk}(E(K)) = \mathrm{rk}(NS(S)) - \mathrm{rk}(T) = \rho - \mathrm{rk}(T)$$

and this implies the corollary.

□

Remark: In the case where $S$ is rational we have

$$b_2 = \rho \tag{3.2}$$

**Theorem 15 (Shioda)** *$T$ is an integral sublattice of $NS(S)$. If we set $L = T^{\perp}$, then $L$ is a negative definite even integral lattice of rank equal to $rk(E(K))$ and determinant given by*

$$\det L = \det NS(S)\,\frac{[NS(S) : L + T]^2}{\det T}$$

*There exists a map (again called $\phi$)*

$$\phi : E(K) \longrightarrow NS(S)_{\mathbf{Q}} = NS(S) \bigotimes \mathbf{Q}$$

*substantially the same as the previous one, with kernel precisely $E(K)_{\mathrm{tor}}$, which enables us to inject $E(K)/E(K)_{\mathrm{tor}}$ into $NS(S)$. Furthermore*

$$Im\,\phi \subset L_{\mathbf{Q}} = L \bigotimes \mathbf{Q}$$

*so that we can make $E(K)/E(K)_{\mathrm{tor}}$ into a positive-definite lattice (not necessarily integral) by defining, for $P$ and $Q$ in $E(K)$, the height pairing*

$$< P, Q >= -(\phi(P).\phi(Q))$$

Remark: $L$ is called the *essential sublattice* of $NS(S)$. These facts follow from a direct knowledge of $\phi$ which also accounts for the explicit formula in part 2 of Main Theorem. We shall see that $L$ is negative-definite. Indeed we can write, by theorem 14:

$$T = U \oplus \bigoplus_{v \in R} T_v$$

where we set

$$U = \mathbf{Z}(O) \bigoplus \mathbf{Z}F$$

and

$$T_v =< \Theta_{v,i} \mid \ (1 \leq i \leq m_v - 1) > \qquad (v \in R)$$

Then $U$ is a unimodular indefinite integer lattice with intersection matrix

$$\begin{pmatrix} -\chi & 1 \\ 1 & 0 \end{pmatrix}$$

Therefore, on $W = U^{\perp} \supset L$, the intersection product is negative definite by the Hodge index theorem ( 13).

Next we ask ourselves whether it is possible to find a sublattice of $E(K)/E(K)_{\text{tor}}$ which is integral. For this purpose we introduce the subgroup of $E(K)$:

$$E(K)^0 \overset{\text{def}}{=} \{P \in E(K) : \ (P) \text{ meets } \Theta_{v,0} \ \forall v \in R\} \tag{3.3}$$

Then $E(K)^0$ is of finite index in $E(K)$. Moreover it is torsion-free so that it can be viewed as a sublattice of $E(K)/E(K)_{\text{tor}}$. Also, the definition of $\text{contr}_v(P,Q)$ implies that, for $P$ or $Q$ in $E(K)^0$, we have

$$< P,Q > \ = \ \chi + (P.O) + (Q.O) - (P.Q) \tag{3.4}$$

$$< P,P > \ = \ 2\chi + 2(P.O) \tag{3.5}$$

Finally, it can be proven that the lattice $E(K)^0$ is even. Let us summarize all this:

**Theorem 16** *$E(K)^0$ defined by 3.3 is a positive-definite integral even lattice of same rank as $E(K)/E(K)_{\text{tor}}$. The height pairing on $E(K)^0$ is given by the formulas 3.4 and 3.5.*

## 3.2 Application to Rational Elliptic Surfaces

Let us apply now the theory to the special case of rational elliptic surfaces and more precisely to the pencil of cubics considered by Shioda.

$\underline{\rho = 10}$: Follows easily from lemma 2 , formulas 3.1 and 3.2 because $C = \mathbf{P}^1$ here.

Therefore from theorem 14 we get:

$$\text{rk}(E(K)) = \text{rk}(E(K)^0) = 8 - \sum_{v \in R} (m_v - 1) \tag{3.6}$$

Now suppose that we take Shioda's pencil of cubics. We have already seen in chapter 2 that all the cubics of the pencil are irreducible, therefore we have in this case $R = \emptyset$ and from 3.3, 3.6:

$$\begin{aligned} E(K) &= E(K)^0 \\ \text{rk}(E(K)) &= \text{rk}(E(K)^0) = 8 \end{aligned}$$

Remark: By integral lattice theory (cf [Ser]) we can say that $E(K) = E(K)^0 \cong E_8$.

## 3.3 Computation of the height matrix of $P_1, \ldots, P_8$

Since $P_i \in E(K) = E(K)^0$, the height pairing is given by the formulas 3.4, 3.5. Since $(P_i) \bigcap (P_j) = \emptyset$ if $i \neq j$ we have

$$\begin{aligned} (P_i.P_j) &= 0 \quad (i \neq j) \\ (P_i.P_j) &= -\chi = -1 \quad (i = j) \end{aligned}$$

and hence

$$\begin{aligned} < P_i, P_j > &= \chi + (P_0.P_i) + (P_0.P_j) - (P_i.P_j) \\ &= \begin{cases} 1 & (i \neq j) \\ 2 & (i = j) \end{cases} \end{aligned}$$

Now the determinant of the height matrix is equal to

$$\det(< P_i, P_j >)_{1 \leq i,j \leq 8} = 9 \neq 0$$

which proves the linear independence of $P_1, \ldots, P_8$ (also, they generate a subgroup of $E(K)$ of index 3).

We refer to [Shio 2] page 113, for the slighty more difficult computation of the height matrix of the eleven points $P_1, \ldots, P_8, M_1, M_2, M_3$.

# Chapter 4

# Explicit formulas and elliptic curves

Riemann in his celebrated 1859 paper first showed the connection between the distribution of the zeros of an $L$ function and the asymptotic behaviour of prime numbers. In view of the standard conjectures connecting algebraic properties of elliptic curves and more generally of abelian varieties to the order of vanishing of the associated $L$ functions, we can recover information about the former by analysing the latter via the "explicit formulas". We refer to [Mes 5] for details.

Let $M$ and $M'$ be two non negative integers, $A$ and $B$ two positive real numbers, $(a_i)_{1\leq i\leq M}$ and $(a'_i)_{1\leq i\leq M}$ two sequences of non negative real numbers such that $\sum_{i=1}^{M} a_i = \sum_{i=1}^{M} a'_i$. Finally, let $(b_i)_{1\leq i\leq M}$ and $(b'_i)_{1\leq i\leq M}$ be two sequences of complex numbers with non negative real part.

Suppose we are given two meromorphic functions $\Lambda_1$ and $\Lambda_2$ verifying the following conditions:

1. There exists a $w \in \mathbf{C}^*$ such that $\Lambda_1(1-s) = w\Lambda_2(s)$.

2. $\Lambda_1$ and $\Lambda_2$ have only a finite number of poles.

3. For $i = 1$ or $2$ $\Lambda_i$ without its singular terms is bounded inside any vertical strip of the form

$$-\infty < \sigma_0 \leq \mathrm{Re}(s) \leq \sigma_1 < +\infty$$

4. There exists $c \geq 0$ such that, for $\mathrm{Re}(s) > 1 + c$ we have:

$$\begin{aligned}\Lambda_1(s) &= A^s \prod_{i=1}^{M} \Gamma(a_i s + b_i) \prod_p \prod_{i=1}^{M'} (1 - \alpha_i(p) p^{-s})^{-1} \\ \Lambda_2(s) &= B^s \prod_{i=1}^{M} \Gamma(a'_i s + b'_i) \prod_p \prod_{i=1}^{M'} (1 - \beta_i(p) p^{-s})^{-1}\end{aligned}$$

   where $p$ runs over all the prime numbers and where $\alpha_i(p)$ and $\beta_i(p)$ are complex numbers of modulus $\leq p^c$.

In what follows we put

$$\begin{aligned}L_1(s) &= \prod_p \prod_{i=1}^{M'} (1 - \alpha_i(p) p^{-s})^{-1} \\ L_2(s) &= \prod_p \prod_{i=1}^{M'} (1 - \beta_i(p) p^{-s})^{-1}\end{aligned}$$

Let

$$F : \mathbf{R} \longrightarrow \mathbf{R}$$

be a function satisfying the following:

1. There exists $\epsilon > 0$ such that

$$F(x) \exp((1/2 + c + \epsilon)x)$$

   is summable and has bounded variation (etc.).

2. $(F(x) - F(0))/x$ has bounded variation.

We also define

$$I(a, b) = a \int_0^{+\infty} (F(ax) e^{-(a/2+b)x} / (1 - e^{-x}) - F(0) e^{-x}/x) dx$$

$$J(a, b) = a \int_0^{+\infty} (F(-ax) e^{-(a/2+b)x} / (1 - e^{-x}) - F(0) e^{-x}/x) dx$$

and

$$\Phi(s) = \int_{-\infty}^{+\infty} F(x) e^{(s-1/2)x} dx$$

**Theorem 17** *In the previous notations we have the formula:*

$$\sum_\rho \Phi(\rho) - \sum_\mu \Phi(\mu) + \sum_{i=1}^{M} I(a_i, b_i) + \sum_{i=1}^{M} J(a'_i, b'_i) =$$

$$F(0)\log(AB) - \sum_{p,i,k\geq 1} (\alpha_i^k(p)F(k\log p) + \beta_i^k(p)F(-k\log p))\frac{\log p}{p^{k/2}}$$

*where $\rho$ (resp. $\mu$) runs over the zeros (resp. the poles) of $\Lambda_1$ in the critical strip $-c \leq Re(z) \leq 1 + c$, each of them counted with multiplicity.*

## 4.1 Application to modular forms

Let $f(z) = \sum_{n\geq 0} a_n e^{2\pi i n z}$ be a modular form for $\Gamma_0(N)$ of weight $k$. In the case where $f$ is a newform, we can apply theorem 17 because it is known that the $L$ function associated to $f$ has an Euler product expansion:

$$L(s,f) = \prod_{p|N}(1 - a_p p^{-s})^{-1} \prod_{p\not| N}(1 - a_p p^{-s} + p^{k-1-s})^{-1}$$

It is known for this function that if

$$\Lambda(s) = (\sqrt{N}/2\pi)^s \Gamma(s) L(s)$$

then

$$\Lambda(s) = C\Lambda(k-s)$$

where $C = \pm 1$. Moreover $\Lambda$ is an entire function, so that after translation, we set

$$L_1(s) = L_2(s) = L(s + \frac{k-1}{2})$$
$$\Lambda_1(s) = \Lambda_2(s) = \Lambda(s + \frac{k-1}{2})$$

Also, in view of Deligne's and Atkin-Lehner results, since $|a_p| \leq 2p^{(k-1)/2}$, we have that $c = 0$ so that the critical strip is $S = [0,1] \times i\mathbf{R}$.

If we choose an even function $F$ satisfying the properties listed above and if we set

$$\begin{cases} b(p^m) = (a_p)^m & \text{if} \quad p|N \\ b(p^m) = \alpha_p^m + {\alpha'_p}^m & \text{if} \quad p\not| N \end{cases}$$

where $\alpha_p$ and $\alpha'_p$ are the roots of $T^2 - a_p T + p^{k-1}$, theorem 17 then reads as:

$$\sum_\rho \Phi(\rho) + 2\sum_{p,m} b(p^m)F(m\log p)\frac{\log p}{p^{mk/2}}$$
$$= F(0)(\log N - 2\log 2\pi) - 2I_F \tag{4.1}$$

where $I_F = I(1,(k-1)/2)$ and $\rho$ runs over the zeros of $L$ translated back by $(k-1)/2$.

## 4.2 Bounding the order of $L$ at $k/2$

Formula 4.1 of the preceding section can be applied to estimate the order $r$ of vanishing of $L$ at $k/2$. Indeed take an even $F$ as before, such that $\mathrm{Re}\Phi$ is positive in the critical strip $S$. Then $F(0)$ is positive and can be assumed to be equal to 1. After rewriting formula 4.1 and dropping all zeros except $1/2$ we obtain:

$$\begin{aligned} r\Phi(\frac{1}{2}) \quad < \quad & \log(k^2N) - 2\log 4\pi + 2\int_0^{+\infty}(1-F(x))/(e^x-1)dx \\ & + 4\sum_{p,m}\frac{F(m\log p)}{p^{m/2}}\log p \end{aligned}$$

For example we may take

$$\begin{cases} F(x) = \frac{1-|x/\log 3|}{\cosh(x/2)} & \text{for} \quad x\in[-\log 3, \log 3] \\ F(x) = 0 & \qquad \text{elsewhere} \end{cases}$$

This gives the following explicit bound:

$$1.072r < \log(k^2N) - 1.97$$

In particular

**Theorem 18** *Let $f$ be a newform of weight $k$ for $\Gamma_0(N)$, and $L$ its associated $L$-function. Then the order $r$ of vanishing of $L$ at $k/2$ is bounded by*

$$r < \log k^2N$$

Assuming the generalized Riemann hypothesis (GRH) we can say more: GRH means that all the zeros of $L$ in the critical strip have real part equal to $k/2$ (or, after normalizing, to $1/2$). Therefore since on the line $\mathrm{Re}(s) = 1/2$ we have

$$\phi(t) = \Phi(\frac{1}{2} + it) = \int_{-\infty}^{+\infty} F(x)e^{itx}dx$$

we need look for functions $F$ having positive Fourier transform.

More precisely, take $F$ positive, even, with support contained in $[-1, 1]$ such that $F(x) \leq 1$ and $F(0) = 1$. For $\lambda > 0$, set $F_\lambda(x) = F(x/\lambda)$. If $\phi_\lambda(t)$ is the corresponding $\phi$ we have $\phi_\lambda(t) = \lambda\phi(\lambda t)$.

As before a little computation shows that

$$\begin{aligned} \lambda r\phi(0) \quad &< \quad \log(k^2N) + 8e^{\lambda/2}\log 3 - 2\log 4\pi \\ & \quad + 2\int_0^{+\infty}(1 - F(x))/(e^x - 1)dx \end{aligned} \tag{4.2}$$

Choosing $\lambda = 2\log\log(k^2N)$ we see that

**Theorem 19** *Under GRH, in the notations of theorem 18, we have*

$$r = O(\frac{\log(k^2N)}{\log\log(k^2N)})$$

*where the constant involved in $O(\ldots)$ is absolute.*

Suppose now that $\phi$ is positive in $[-1, 1]$ and negative elsewhere (this can be done). Then if $t_0 > 0$ is the first zero of $L$ on the line $\mathrm{Re}(s) = 1/2$ distinct from $1/2$ and if $\lambda = 1/t_0$, then we obtain the lower bound:

$$\lambda r\phi(0) > \log k^2N - O(e^{\lambda/2})$$

which together with theorem 19 gives

**Theorem 20** *If $t_0$ is as before, we have*

$$t_0 = O(\frac{1}{\log\log k^2N})$$

*where again the constant involved in $O(\ldots)$ is absolute.*

## 4.3 Application to elliptic curves

The results of the preceding section apply well to find upper bounds on the rank of an elliptic curve over $\mathbf{Q}$ because of the Taniyama-Shimura-Weil conjecture saying that the $L$-function of an elliptic curve over $\mathbf{Q}$ arises as the $L$-function attached to a certain modular form of weight 2 and level equal to the conductor $N$ of the elliptic curve $E/\mathbf{Q}$, and the Birch and Swinnerton-Dyer conjecture that tells us that $r$ is precisely the rank of $E(\mathbf{Q})$.

However, given $E/\mathbf{Q}$, we can refine our estimate of $b(p^m)$ for that specific curve and obtain better results using formula 4.1. Indeed, put in that formula as $F$ the Odlysko function (cf [Mes 5]). In particular, since the main contribution comes from $b(p) = a_p = p + 1 - N_p$, we need only compute the number $N_p$ of points of the reduced curve mod $p$ for $p \leq e^{\lambda}$.

Example: For the curve 11B we get the estimate $0 = r \leq 0.0014$, for 189F $0 = r \leq 0.430$, for 200C $1 = r \leq 1.011$. Here we took $\lambda = \log 23$ which is pretty small!

Notice also that if we proceed as in the previous section, where we made the crude estimate $|b(p^m)| \leq 2p^{m/2}$, we still obtain with $\lambda = \log 100$

$$r < 0.268 \log N + 1.03$$

which is not bad for small $N$.

The precision of such an estimate seems to arise from the fact that in the best examples we have $t_0 \approx 1/\log N$, so that the first non-real zero of $L$ in the critical strip is "sufficiently far" from $k/2$. We now turn to indicate a sufficient condition under which this holds.

Let $f$ be a newform of weight $k$ for $\Gamma_0(N)$. Then $f$ is real on $i\mathbf{R}^+$, so that the following definition makes sense:

**Definition 2 (Mazur, Swinnerton-Dyer)** *A critical fundamental point of odd order (cfpoo) of $f$ is a complex number of the form it with $t$ positive such that $f$ changes sign.*

**Theorem 21 (Mazur, Swinnerton-Dyer)** *If $h$ is the number of cfpoo's of $f$ we have*

$$r \leq h \quad \textit{and} \quad r \equiv h \pmod 2$$

Actually among all curves with conductor $\leq 430$, only 17 fail to have $r = h$ for their associated $L$-function. This leads us to the following:

**Theorem 22** *Suppose in the above that $r = h$. Then if $s$ is a zero of $L$ distinct from $k/2$, we have*

$$|s - (k/2)| > \frac{1}{10 \log(kN)}$$

Remark:

1. Notice that the theorem is unconditional of GRH.

2. The experimental results of Fermigier show that there is a strong evidence that the first non-real zero has an ordinate of $C/\log N$ (case of elliptic curves, $k = 2$). Moreover, $C$ seems to grow as the rank grows. Question: does $C$ go to infinity as the rank grows?

### 4.3.1 Twists with high rank

Let $E/\mathbf{Q}$ be an elliptic curve. It seems reasonable to ask ourselves if for any $M > 0$, there exists a quadratic twist $E_\chi$ of $E$ such that $\mathrm{rank}(E_\chi(\mathbf{Q})) > M$. We can at least bring an evidence of affermative answer.

**Theorem 23** *Let $f$ be a newform of weight $k$ for $\Gamma_0(N)$. Then, for any $M$, there exists a quadratic twist $f_\chi$ of $f$ such that $M$ is smaller than the number of cfpoo's of $f_\chi$.*

### 4.3.2 Curves with high rank

Examining formula 4.1, we see that in order for $E(\mathbf{Q})$ to possibly have a high rank, we should require that $-b(p) = -a_p$ be as large as possible, i.e. we want $N_p$ as large as possible ($N_2 = 5,\ N_3 = 7,\ N_5 = 10\ldots$). If we go up to $p = 41$, we get a curve of rank 14, namely the curve whose coefficients in Weierstraß form are

$$[0, 2597055, 357573631, -549082, -19608054]$$

In general, the most effective method to find elliptic curves over $\mathbf{Q}$ with exceptionally high rank is this one, applied to the curves of rank at least 11 obtained in 5.1 and following. Fermigier ([Ferm 1]) thus finds a curve of rank 19, while Kouva and Nagao ([KN]) go up to 21 and Fermigier (unpublished) obtains 22 (May 1996).

## 4.4 An interesting question

Take the curve

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

over $\mathbf{Q}(t)$. It has rank 0. By specialisation, we find that the proportion of curves having rank 0 is 0.40, rank 1 is 0.35, rank 2 is 0.1 etc.

Question: Is there a positive proportion for each rank?

Also the curve over $\mathbf{Q}(t)$

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

is of rank 1. Again by specialisation, there are 40% of curves of rank 1, 35% of curves of rank 2, 10% of rank 3 etc.

The generalisation is clear.

**Question 1** *Let $y^2 = x^3 + a(t)x + b(t)$ be an elliptic curve over $\mathbf{Q}(t)$ of rank $r$. Then by specialisation roughly 40% of curves are of rank $r$, roughly 35% of rank $r+1$, roughly 10% of rank $r+2$ etc.*

We refer to [Ferm 2] for numerical results concerning this question.

## 4.5 An application to algebraic varieties

Let $A/\mathbf{Q}$ be an algebraic variety of dimension $d$ and conductor $N$. We can attach to it an $L$-function $L$. If we assume that $L$ satifies the standard conjectures then by the aforementioned methods we find a lower bound for its conductor.

**Theorem 24** *Suppose that $L$ has analytic continuation to an entire function and that the function*

$$\Lambda(s) = N^{s/2}((2\pi)^{-s}\Gamma(s))^d L(s)$$

*satisfies the functional equation $\Lambda(s) = \pm\Lambda(2-s)$ and is entire of order 1. Then we have the lower bound $N > 10.32^d$. In particular, $A$ cannot have good reduction everywhere.*

This raises the question of the minimality of the conductor for an abelian variety over $\mathbf{Q}$ of dimension $d$. For $d = 1$ (elliptic curve) the theorem says that $N > 10$ and indeed for $N = 11$ we have $X_0(11)$. For $d = 2$ we have that $X_0(11) \times X_0(11)$ has conductor $11^2 = 121$. The bound of the theorem gives $N \geq 109$ but so far we don't know of any $A$ such that $109 \leq N < 121$.

In general, does there exist an $A$ of dimension $d$ such that $10.32^d \leq N < 11^d$ ? And if not, is $(X_0(11))^d$ the minimal one ? :wq

# Chapter 5

# Curves of high rank

In this chapter we will exhibit elliptic curves of rank 11 and 12 over $\mathbf{Q}(t)$.

## 5.1 Curves of rank 11

We begin with a lemma analogous to lemma 1.

**Lemma 3** *Let $k$ be a field with $\operatorname{char} k \neq 3$ and $p$ a monic polynomial of degree $3n$ in $k[x]$. Then there exists a unique triplet $(g, r, s) \in (k[x])^3$ with $g$ monic of degree $n$, $\deg r \leq n-1$ and $\deg s \leq n-1$ such that*

$$p = g^3 + rg + s$$

Proof: Again this is proved in the same way as in lemma 1. Another way of seeing it is that $g$ is the polynomial part of $p^{1/3}$ which is computed using the binomial expansion $(1+x)^{1/3} = 1 + x/3 + \cdots$ valid in characteristic different from 3. Then a rapid computation shows that $\deg p - g^3 \leq 2n-1$ which proves the theorem (uniqueness again follows from the binomial expansion).

□

Now take in the preceding lemma $n = 4$. As in chapter 1 we take a polynomial

$$p(x) = \prod_{i=1}^{12} (x - x_i) \ \ (x_i \in k)$$

Define $(g, r, s)$ as in lemma 3. Then the curve $C$ given by

$$y^3 + yr(x) + s(x) = 0$$

has $P_i = (x_i, g(x_i)) \in C(k)$ but its genus is 3 in general. However if $\deg r \leq 2$ then $C$ is a cubic therefore in general of genus 1.

Therefore we want to take $k = \mathbf{Q}(t)$ and $p$ such that:

1. $\deg r \leq 2$.

2. $C$ is a non singular cubic of non-constant modular invariant.

3. The points $P_i$ are linearly independent in $\mathrm{Pic}(C)$.

Then choosing $P_{12}$ for example as the origin we find an elliptic curve over $\mathbf{Q}(t)$ of rank $\geq 11$.

Call $r_5 = r_5(x_1, \ldots, x_{12})$ the coefficient of degree 3 of $r$. Then since $p$ is a homogeneous polynomial in $x, x_1, \ldots x_{12}$, it is easy to see that $r_5$ is a homogeneous symmetrical polynomial of degree 5 in the $x_i$'s. Call $X = (x_1, \ldots, x_{12})$.

**Lemma 4** *1. If $u$ is a free variable, then $r_5(X + (u, \ldots, u)) = r_5(X)$.*

*2. If $p$ is the cube of a polynomial, then $r_5(X) = 0$.*

*3. If $p$ is an even polynomial, then $r_5(X) = 0$.*

Proof:

1. Follows from the uniqueness in lemma 3.

2. Same thing, because $r = s = 0$.

3. Again using uniqueness we write

$$p(x) = q(x^2) = g^3(x^2) + g(x^2)r(x^2) + s(x^2)$$

where we apply lemma 3 to $q$ of degree 6, so that $\deg g \leq 2$, $\deg r \leq 1$ and $\deg s \leq 1$. Therefore by uniqueness $g(x^2)$, $r(x^2)$ and $s(x^2)$ are the corresponding polynomials for $p$ and looking at degrees we are done.

□

**Lemma 5** *Let $a, b, c, d$ be four indeterminates. Then the point*

$$V = (a, b, c, d, a, b, c, d, a, b, c, d)$$

*is a double point of $r_5(X) = 0$.*

Proof: We already showed that $r_5(V) = 0$. We are to show that if $D = (1, 0, \ldots, 0)$, then $r_5(V + \epsilon D)$ as a function of $\epsilon$ is divisible by $\epsilon^2$. The same reasoning will apply to the other variables and the proof will be complete. Now let

$$\begin{aligned} p_\epsilon(X) &= (X - a + \epsilon)(X - a)^2(X - b)^3(X - c)^3(X - d)^3 \\ &= (1 + \frac{\epsilon}{X - a})(X - a)^3(X - b)^3(X - c)^3(X - d)^3 \end{aligned}$$

Since $g_\epsilon$ is the polynomial part of $p_\epsilon^3$, we see that

$$g_\epsilon \equiv (X - a + \frac{\epsilon}{3})(X - b)(X - c)(X - d) \qquad (\text{mod } \epsilon^2)$$

so that

$$p_\epsilon - g_\epsilon^3 \equiv 0 \qquad (\text{mod } \epsilon^2)$$

and therefore $r_\epsilon$ and $s_\epsilon$ are divisible by $\epsilon^2$ and so is the leading coefficient $r_5(V + \epsilon D)$ of $r_\epsilon$ .

□

**Lemma 6** *In the hypothesis of lemma 5, let $t$ be an indeterminate and*

$$W = (d, d, d, c, c, c, b, b, b, a, a, a)$$

*Then $r_5(V + tW) = 0$.*

Proof: $r_5(t_1 V + t_2 W)$ is a homogeneous polynomial of degree 5 in $(t_1, t_2)$ which has the two double roots $(0, 1)$ and $(1, 0)$ by lemma 5. To show the lemma it suffices then to produce two new roots of that polynomial. One is $V - W$ because its components are the roots of an even $p$ and the other is $V + W$ because the $p$ corresponding to $V + W - ((a + b + c + d)/2, \ldots, (a + b + c + d)/2)$ is even and because of lemma 4.

□

To sum up, given $a, b, c, d$ four rational numbers, we can apply lemma 4 to the polynomial whose roots are the components of $V + tW$ to obtain an elliptic surface $C$ (i.e. a cubic over $\mathbf{Q}(t)$). We should expect $C$ in general to be nonsingular.

**Example**: In [Mes 2] we specialize $a, b, c, d$ in $-1, 0, 2, 11$. The corresponding $C$ is given and also the twelve points $P_i$. In fact $C$ is an elliptic surface in the sense of [Shio 2], hence we can apply the methods described therein to compute the height matrix. Since the only singular fibers are irreducible (Kodaira $I_1$) we have $E(\mathbf{Q}(t))^0 = E(\mathbf{Q}(t))$ (cf chapter 3) and the height matrix has integer entries. Lemma 7 of [Mes 2] shows how to compute $< P_i, P_j >$.

We find that the height matrix has determinant $2^{16}3^4$, thus the twelve points $P_i$ are independent in $\mathrm{Pic}(C)$.

### 5.1.1 Another way to find rank 11

Instead of using lemma 3, we can apply lemma 1 to $p$ of degree 12 to obtain $p = g^2 - r$, where $\deg r \leq 5$. Therefore the curve $C$ given by $y^2 = r(x)$ contains the points $P_i = (x_i, g(x_i))$ where $x_i$ runs over the roots of $p$. However $C$ is of genus 2 in general but if $\deg r \leq 4$, then $C$ is of genus 1.

Now if $p$ is of the form $q(x-t)q(x+t)$, then the leading coefficient of $r$ is equal to $t^2\times$ a constant. By the above methods we can make this constant equal to zero. This is the case if $q(x) = (x+17)(x+16)(x-10)(x-11)(x-14)(x-17)$ and the twelve points $P_i$ are again found to be independent by the usual methods.

## 5.2 Curves of rank 12

We can push further the previous two constructions to find a thirteenth point in $\mathbf{Q}(t)$ independent of the first twelve.

### 5.2.1 First construction

The trick is always to find a relation between $a, b, c, d, t$ to produce an extra rational point by solving algebraic equations.

Here we take $P_1 = (x_1, y_1)$ and look at the two other points on $C$ having abscissa $x_1$. These points may not be defined a priori in $\mathbf{Q}(a, b, c, d, t)$. Nevertheless their ordinates satisfy the equation

$$y^3 + r(x_1)y + s(x_1) = 0$$

Since $y_1 \in \mathbf{Q}(a,b,c,d,t)$ they also satisfy the equation

$$y^2 + \alpha y + \beta \tag{5.1}$$

where $\alpha = y_1$ and $\beta = y_1^2 + r(x_1)$. It is not difficult to see that $\tilde{\Delta}(t) = \alpha^2 - 4\beta = t^2\Delta(t)$, where $\Delta$ is a polynomial of degree at most 4. Since at $t = 0$, $P_1, P_5$ and $P_9$ all have abscissa $x_1(0)$, a change of variables implies that $\Delta(0)$ is a square in $\mathbf{Q}(a,b,c,d)$. [1]

Therefore we can write $\Delta$ in the form

$$\Delta(t) = (v + v_1 t + v_2 t^2)^2 + t^3(w_0 + u_0 t)$$

and we see that for $t = -w_0/u_0$, $\Delta$ is always a square and the two roots of 5.1 are rational over $\mathbf{Q}(a,b,c,d)$, giving the three points $P_1, Q, \tilde{Q}$.

**Example**: Fix $a = -1, b = 0, c = 2$. Then $t$ is a rational function in $d$, so that now $C$ is an elliptic curve over $\mathbf{Q}(d)$ with 12 independent points in $C(\mathbf{Q}(d))$, namely (choosing $P_{12}$ as the origin) $P_1, \ldots, P_{11}, Q$, as we readily show by standard methods.

### 5.2.2 Second construction

In the previous section we showed how to construct an elliptic curve $C$ over $\mathbf{Q}(t)$ of rank 11 and of the form $y^2 = r(x)$, where $\deg r = 4$. In the specific example we gave, the leading coefficient of $r$ was $429t^2 + 53260$. Now it is known (see for instance [Silv]) that we can embed $C$ in $\mathbf{P}^3$ and that it has two points at infinity rational over $\mathbf{Q}(\sqrt{429t^2 + 53260})$.

Now the non degenerate conic $K$ given by $429t^2 + 53260 = u^2$ is $\mathbf{Q}$ - isomorphic to the projective line, because $(3, 239) \in K(\mathbf{Q})$. Therefore if $z$ parametrizes $K$, we get that $C$ as an elliptic curve over $\mathbf{Q}(z)$ has two new rational points. If we take one of them as origin, then the $12 \times 12$ height matrix of the points $P_i$ has determinant equal to $2^{26}3^6 5 \neq 0$, thus proving that $\mathrm{rank}(C(\mathbf{Q}(z))) \geq 12$.

**Corollary 3** *There exist infinitely many elliptic curves defined over* $\mathbf{Q}$ *with rank* $\geq 12$*.*

[1] in fact $C$ is isomorphic to a curve for which $\tilde{\Delta} = \Delta$ but with abscissae left unchanged

## 5.3 Nagao-Mestre construction of rank 13

We can give a quick outline of how to proceed in order to construct a two parameter family of elliptic curves over $\mathbf{Q}(w)$ of rank at least 13, generalizing Nagao's result in [Nag 1] who found one curve (defined over $\mathbf{Q}(t)$) belonging to this family.

We proceed as in the second method for obtaining curves of rank 11: we take $p = g^2 - r$, where $p$ is of degree 12 and $r$ of degree 4.

Choose $p_6$ of degree 6 with roots $x_1, \ldots, x_6$ and let $p(x) = p_6(x-t)p_6(x+t)$. The curve $y^2 = r(x)$ then has the twelve rational points $(x_i \pm t, g(x_i \pm t))$. We try to find $p_6$ such that there is another rational point of abscissa $a + bt$.

This means that $r(a + bt) = s(t)^2$, where $s$ is a polynomial. Thus we must have

$$p(a + bt) = g^2(a + bt) - s^2(t) = (g(a + bt) - s(t))(g(a + bt) + s(t)) \tag{5.2}$$

Take $p_6$ to be of the form $p_6 = p_2 q_2 p_1 q_1$, where

$$\begin{cases} p_2(x) = x^2 + a_1 x + a_0 \\ q_2(x) = x^2 + x + b_0 \\ p_1(x) = x + c_0 \\ q_1(x) = x - c_0 - a_1 - 1 \end{cases}$$

If we let

$$\begin{aligned} R(x) = 2g(x) &- p_2(x-t)p_2(x+t)p_1(x-t)q_1(x+t) \\ &- q_2(x-t)q_2(x+t)p_1(x+t)q_1(x-t) \end{aligned}$$

Then solutions to the equation

$$S(t) = R(a + bt) = 0 \tag{5.3}$$

will give rise to a rational point on $y^2 = r(x)$ with abscissa $a + bt$, by 5.2 . Note that equation 5.3 is of degree 4 in $t$. Choosing $a_0, c_0$ carefully will set to zero the coefficients of degree 0 and 4 (hence 1 and 3) of $S$. Also for a specific choice of $b_0$ the coefficient of degree 2 vanishes. Thus $a + bt$ is a root of 5.3 now.

Next we know that $\deg r = 5$ so that we want to impose that its leading coefficient be zero. This coefficient is a product of two affine terms in $a$; one doesn't fit ($r$ is then a perfect square) but the other one is good. $a$ is then fixed and we still have a freedom of choice for $b$ and $a_1$.

We now impose that the discriminants of $p_2$ and $q_2$ be perfect squares, which gives the equation of a quadric with a rational point, hence we can parametrize $b = b(u,v)$ and $a_1 = a_1(u,v)$.

Now the curve $y^2 = r(x)$ defined over $\mathbf{Q}(u,v,t)$ has 13 rational points.

In order to find another, to be taken as origin, note that the degree 4 coefficient of $r$ is of the form $q(u,v)^2t^2+m(u,v)$ (miracle!?). Hence the conic $q(u,v)^2t^2+m(u,v) = z^2$ can be parametrized over $\mathbf{Q}$ (we have two rational points at infinity) and if $t = t(u,v,w)$, then the curve $y^2 = r(x)$ gets two new points at infinity, defined over $\mathbf{Q}(u,v,w)$.

Choosing one of them as origin of the curve $y^2 = r(x)$, we get an elliptic curve with 13 points defined over $\mathbf{Q}(u,v,w)$, i.e. a family of elliptic curves over $\mathbf{Q}(w)$ depending on two parameters. To prove that these 13 points are independent, we can specialize and use PARI (the curve found by Nagao in [Nag 1] was a specialization in $u,v$ of this one).

## 5.4 Curves of rank $\geq 14$ defined over $\mathbf{Q}(t)$

¿From the preceding curve, using similar constructions, one can find:

**Theorem 25 (Mestre, April 1996)** *There exists an elliptic curve defined over $\mathbf{Q}(t)$ of rank $\geq 14$.*

# Chapter 6

# Curves of high rank and constant $j$

We have already mentioned the folklore conjecture according to which the rank of elliptic curves over $\mathbf{Q}$ is unbounded. Also we mentioned a stronger conjecture: let $E/\mathbf{Q}$ be an elliptic curve. Is the rank of quadratic twists of $E$ bounded?

Remark: It would be so if a conjecture of Honda were true. Note also that this contrasts with the previous approach using critical fundamental points of odd order.

Let's recall a definition.

**Definition 3** *Let $E/\mathbf{Q}$ be an elliptic curve given by $y^2 = x^3 + ax + b$. For $d \in \mathbf{Q}$ we define the elliptic curve $E_d$ given by $dy^2 = x^3 + ax + b$ to be the twist of $E$ by $d$.*

Remarks:

1. It is known that $j(E_d) = j(E)$ (cf. [Silv]).

2. If $j(E) \neq 0,\ 1728$, then

$$E \cong_{\mathbf{C}} E' \Longrightarrow \exists d \in \mathbf{Q} \ : \ E' \cong_{\mathbf{Q}} E_d$$

3. If $k = \mathbf{Q}(\sqrt{d})$ then $E(k)$ is related to $E(\mathbf{Q})$ and $E_d(\mathbf{Q})$ in the following way: let $\sigma$ be a generator of $\mathrm{Gal}(k/\mathbf{Q})$ and define an application

$$\begin{array}{ccc} E(k) & \xrightarrow{\phi} & E(\mathbf{Q}) \\ P & \longmapsto & P + P^{\sigma} \end{array}$$

If we write $E$ in Weierstraß form, then it is easy to characterize $\ker \phi$. Indeed

$$P^\sigma = -P \iff \left\{ \begin{array}{rcl} x^\sigma & = & x \\ y^\sigma & = & -y \end{array} \right.$$
$$\iff \left\{ \begin{array}{rcl} x & \in & \mathbf{Q} \\ y & = & u\sqrt{d}\ (u \in \mathbf{Q}) \end{array} \right.$$

i.e. we have the exact sequence

$$0 \longrightarrow E_d(\mathbf{Q}) \longrightarrow E(k) \xrightarrow{\phi} E(\mathbf{Q}) \longrightarrow \text{coker}\phi \longrightarrow 0$$

Since $2E(\mathbf{Q}) = \phi(E(\mathbf{Q})) \subset \phi(E(k))$ and because of the weak Mordell-Weil theorem, we have that coker$\phi$ is finite, leading to the relation

$$\text{rk}E(k) = \text{rk}E(\mathbf{Q}) + \text{rk}E_d(\mathbf{Q})$$

The goal of this chapter is to find an infinity of elliptic curves $E/\mathbf{Q}$ of large rank but of constant modular invariant $j$. For this purpose we will make use of twists.

Let us notice first that it is relatively easy to find infinitely many twists of $E$ with rank $\geq 1$. Indeed let $E$ be given by $y^2 = x^3 + ax + b$ and take any $x_0 \in \mathbf{Q}$. If $d = x_0^3 + ax_0 + b$ is not a square then it is not difficult to show that the point $(x_0, 1) \in E_d(\mathbf{Q})$ is of infinite order.

Next we have the general

**Theorem 26 (Mazur-Gouvêa)** *Let $E/\mathbf{Q}$ be an elliptic curve. Suppose Taniyama-Shimura-Weil and Birch Swinnerton-Dyer conjectures hold. Then for any $\epsilon \geq 0$ there exists a constant $C_\epsilon$ such that*

$$\#\{d \in \mathbf{Z} \textit{ with } |d| \leq M \textit{ and } r_a(E_d) \geq 2\} \geq C_\epsilon M^{\frac{1}{2}-\epsilon}$$

We will show that

**Theorem 27** *For any $j \in \mathbf{Q}$ there exist infinitely many $E/\mathbf{Q}$ such that*

- *$j(E) = j$*
- *rk$E(\mathbf{Q}) \geq 2$.*

**Theorem 28**

- *If $j = 0$ then there exist infinitely many $E/\mathbf{Q}$ with $j(E) = 0$ and rk$(E(\mathbf{Q})) \geq 6$.*

- *If $j = 1728$ then there exist infinitely many $E/\mathbf{Q}$ with $j(E) = 1728$ and $rk(E(\mathbf{Q})) \geq 4$.*

**Definition 4** *Let $C$ be an algebraic curve and $E$, $E'$ two curves of genus 1. Given two morphisms $p : C \to E$ and $p' : C \to E'$, we say that they are independent if the pull-backs of differentials of the first kind on $E$ and $E'$ respectively by $p$ and $p'$ are independent.*

**Theorem 29** *Let $k$ be a field of characteristic zero and $j \in k$. Then there exist a quadratic covering $C$ of $\mathbf{P}^1$ defined over $k$ and an elliptic curve $E$ defined over $k$ with invariant $j$ together with two independent morphisms $p, p' : C \to E$ defined over $k$.*

*(or equivalently, there exist $C$, $E$ and an abelian variety $A$ such that $E \times E \times A$ is isogenous to $Jac C$).*

**Theorem 30** *Let $j \in k$. There exists an elliptic curve $E/k(t)$ with invariant equal to $j$ and rank at least 2, not isomorphic over $k(t)$ to a constant curve.*

It is clear that theorem 30 implies theorem 27. To prove theorem 29 we first prove

**Theorem 31** *Let $E/k$ and $E'/k$ be two elliptic curves. Suppose that $j(E)$ and $j(E')$ are not simultaneously equal to 0 or 1728. Then there exists a quadratic covering $C/k$ of $\mathbf{P}^1$ together with two independent morphisms $p : C \to E$ and $p' : C \to E'$ defined over $k$.*

Proof: Take two equations $y^2 = x^3 + ax + b = f(x)$ and $y^2 = x^3 + a'x + b' = g(x)$ defining $E$ and $E'$ respectively. The assumption made on $j(E)$ and $j(E')$ implies $a = 0 \Rightarrow a' \neq 0$ and $b = 0 \Rightarrow b' \neq 0$. If $u$ is an unknown, the equation (in $x$)

$$u^6 f(x) = g(u^2 x)$$

has the solution

$$x = h(u) = -\frac{b' - u^6 b}{u^2(a' - u^4 a)}$$

Now define $C$ by the equation $Y^2 = f(h(X))$. Define also the two morphisms

$$\begin{array}{rcl} p : C & \longrightarrow & E \\ (X, Y) & \longmapsto & (h(X), Y) \\ & \text{and} & \\ p' : C & \longrightarrow & E' \\ (X, Y) & \longmapsto & (X^2 h(X), X^3 Y) \end{array} \tag{6.1}$$

If $\omega = p^*(dx/y)$ and $\omega' = p'^*(dx/y)$ then by direct computation

$$\frac{\omega}{\omega'} = \frac{3aX^4b' - 2X^6ba' - b'a'}{X^3(X^6ba - 3X^2ba' + 2ab')}$$

which is a non-constant rational function, thereby proving theorem 31.

□

Proof of theorem 29: If $j \neq 0,\ 1728$, theorem 29 follows immediately from theorem 31 because for any $j \in k$, there exists a $E/k$ of invariant $j$.

If $j = 0$, then choose as $C$ the curve of equation $y^2 = x^6 + 1$. Then if $E$ is the elliptic curve of invariant 0 defined by $y^2 = x^3 + 1$, we have $\mathrm{Jac}\, C$ is $\mathbf{Q}$-isogenous to $E \times E$ and we're done.

If $j = 1728$, we let $C$ be the curve $y^2 = (t^2+1)(t^2-2)(2t^2-1)$. The two morphisms $(t, y) \mapsto (t^2, y)$ and $(t, y) \mapsto (1/t^2, y/t^3)$ define coverings of $C$ onto the elliptic curve $y^2 = (x+1)(x-2)(2x-1)$ which has invariant equal to 1728, thereby proving our theorem.

□

Theorem 29 implies theorem 30: There is a general proof of this fact given in [Mes 7] but we can give here a proof "ad hoc" in the case where $j \neq 0,\ 1728$. In this case formulæ 6.1 imply that, if we call $P = (t, \sqrt{f(t)})$ where $f$ is as in the proof of theorem 31, then

$$p(P)^\sigma = -p(P) \text{ and } p'(P)^\sigma = -p'(P)$$

where $< \sigma >= \mathrm{Gal}(k(\sqrt{f(t)})/k)$. By the exact sequence above we conclude that

$$(p(P), p'(P)) \in E_{f(t)}(k(t)) \times E_{f(t)}(k(t))$$

so that they are rational points of a curve of constant invariant $j(E)$. Since by construction $p$ and $p'$ are independent, we have that $p(P)$ and $p'(P)$ are independent in $E(k(\sqrt{f(t)}))$ (or in $E_{f(t)}(k(t))$), because otherwise if $mp(P) + np'(P) = 0$ we would get

$$mp^*(\omega_P) + np'^*(\omega_P) = 0$$

where $\omega$ is a differential of the first kind on $E$ and by the invariance of $\omega$ this contradicts the independence of $p$ and $p'$.

For $j = 0,\ 1728$ we refer to what follows.

□

Proof of theorem 28:

**Case** $j=1728$: Let $p(x)=x^4+a_2x^2+a_1x+a_0\in k[x]$, with roots $x_i\in k$ ($\sum_{i=1}^4 x_i=0$). The curve $E$ of equation $x^4+a_2y^2+a_1y+a_0=0$ has the four $k$-rational points $P_i=(x_i,x_i)$. If

$$a_0=-u^4 \quad (u\in k) \tag{6.2}$$

then $O=(-u,0)\in E(k)$. If $a_2(a_1^2-4a_0a_2)\neq 0$ then $E$ is $k(t)$-isomorphic to $y^2=x^3+a_2(a_1^2-4a_0a_2)x$, therefore is an elliptic curve of modular invariant 1728.

Now equation 6.2 is equivalent to

$$x_1x_2x_3(x_1+x_2+x_3)=u^4$$

As is pointed out in [Di], Euler studied this surface and found several rational curves on it, for instance

$$u=1,\qquad x_1=t\frac{2t^2-1}{2t^2+1},\qquad x_2=\frac{2t^2-1}{2t(2t^2+1)},\qquad x_3=\frac{4t}{2t^2-1}$$

If we form the polynomial $p$ as above from these data, we obtain $E/k(t)$ of invariant 1728. To show that it is not isomorphic to a constant curve it suffices to apply the usual formulæ. For example since

$$\frac{a_2(a_1^2-4a_0a_2)(t)}{a_2(a_1^2-4a_0a_2)(t_0)}$$

is not a fourth power in $k(t)$ ($t_0$ is just a value of of $t$) we are done. Choose $O$ as origin, then the four points $P_i$ are independent, as we see by specialization, using PARI.

**Case** $j=0$: Again take $p$ of the form

$$p(x)=x^6+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0=\prod_{i=1}^{6}(x-x_i)$$

with $x_i\in k$ and apply lemma 3 to $p$. Call $R=p-g^3$ so that $\deg R\leq 3$. Then the curve $E$ of equation $y^3+R(x)=0$ contains the six $k$-rational points $P_i=(x_i,g(x_i))$. We still have to find one more $k$-rational point to be put as the origin. Notice that if the discriminant $D$ of $R$ is not zero, then $E$

is a nonsingular curve of genus 1 isomorphic to $y^2 = x^3 - 16D$ therefore of invariant 0.

If the leading coefficient of $R$ is a cube in $k$, then at least one point at infinity is rational over $k$ and we can set it to be the origin $O$ of the elliptic curve $E$.

We have $r(x) = a_3x^3 + \cdots$. Since $a_3$ is a homogeneous polynomial of degree 3 in the $x_i$'s, we get that $u^3 = a_3$ is the equation of a cubic hypersurface $H$ (in the variables $u$ and $x_i$ $1 \leq i \leq 5$). This surface has a lot of rational points on it and we can find non trivial rational curves by standard methods (see [Elk], for example take a plane $P$ tangent to $H$. Then $H \cap P$ is a cubic with a singular point, i.e. birational to $\mathbf{P}^1$). For example

$$\begin{aligned}
x_1 &= -126(35t-19)(14t-13)(t+1)\\
x_2 &= 63(-980t^3+3549t^2-3084t+1135)\\
x_3 &= x_1\\
x_4 &= 63(1127t^3-3108t^2+3525t-988)\\
x_5 &= -113876t^3+265629t^2-259980t+69103\\
x_6 &= -x_1-x_2-x_3-x_4-x_5
\end{aligned}$$

Again by standard methods since $D(t)/D(t_0)$ is not a sixth power in $k(t)$ we have that $E$ is not $k(t)$-isomorphic to a curve defined over $k$. The independence of the six points $P_i$ is dealt with as previously.

□

## 6.1 Curves of rank 7 with $j = 0$

We now prove that there exist infinitely many elliptic curves defined over $\mathbf{Q}$ with modular invariant equal to zero and Mordell-Weil rank at least 7. Again this follows using the usual arguments from the following theorem:

**Theorem 32** *Let $v$ be a variable. There exists an elliptic curve defined over $\mathbf{Q}(v)$ with zero invariant, not $\mathbf{Q}(v)$-isomorphic to an elliptic curve defined over $\mathbf{Q}$ and rank at least 7.*

Proof: The proof follows the same lines as for rank 6. Take $p \in \mathbf{Q}(x)$ of the form $\prod_{i=1}^{6}(x - x_i)$ and write it as $p = g^3 - r$ where $g$ is monic of degree 2 and $\deg r \leq 3$. Then the curve of equation $y^3 = r(x)$ is usually an elliptic curve of invariant 0 having the 6 rational points $(x_i, y_i)$, where $g(x_i) = y_i$.

As before we will produce a seventh rational point (at infinity). The other new rational point will come out of a rational solution of $y_1^3 - r(x) = 0$, different from $x_1$. We have already seen a similar trick in section 5.2.

Take the five unknowns $t, a, b, c, d$ and let $x_i = (u_i + tv_i)$ $(1 \leq i \leq 6)$ where

$$\begin{cases} (u_1, \ldots, u_6) & = & (a, a, b, c, d, -2a - b - c - d) \\ (v_1, \ldots, v_6) & = & (1, -1, 1, -1, 1, -1) \end{cases}$$

Then $p$ is a homogeneous polynomial in $t, a, b, c, d, x$ of degree 6. If we write

$$r(x) = \sum_{i=0}^{3} r_i x^i \tag{6.3}$$

then we see that $r_3$ is homogeneous of degree 3 in $t, a, b, c, d$. Moreover, working on the symmetries of $p$, it can be easily shown that $\deg_t r_3 \leq 1$ (for example the term with $t^3$ is zero because if we set $a = b = c = d = 0$ then $p$ becomes a cube so that $r = 0$). Likewise

$$\deg_t r_{3-i} \leq 1 + i \qquad (0 \leq i \leq 3) \tag{6.4}$$

Also the leading coefficient of $r_3$ (seen as polynomial in $t$) is a polynomial of degree 1 in $d$, namely

$$4a^2 + 2c^2 + 4ab + 2bc + 4ca + 2dc + 2db + 4da$$

Hence for a suitable $d$ we have that $r_3$ doesn't depend on $t$ anymore. Explicitly

$$r_3 = \frac{2a(b+c)(a+b)(a+c)}{b+c+2a}$$

Next we try to impose that one of the three points at infinity be rational. We want to parametrize $a, b, c$ so that $r_3$ becomes a cube. For example we can notice that on the surface $r_3(a, b, c) = -1$ we can find rational curves like

$$a = -\frac{(v-1)(v^2+v+1)}{4v}, \qquad b = -\frac{v^3+3}{4v}, \qquad c = \frac{v^6 - 6v^3 - 3}{(4v-4)(v^2+v+1)v}$$

Until now we have defined a curve $y^3 = r(x)$ over $\mathbf{Q}(v, t)$ with 7 rational points.

We are looking for a new rational point of ordinate $y_1$. This amounts to finding solutions of

$$h(x) = \frac{r(x) - r(x_1)}{x - x_1} = 0$$

Now the discriminant $D$ of $h$ is a polynomial of degree 4 in $t$ and its leading coefficient $m$ is a square in $\mathbf{Q}(v)$, as can be readily checked using 6.4. Explicitly we have

$$\begin{aligned} m = 16v^4(v^{12}+14v^6+1)^2 \times \\ (v^6+3)^2(v-1)^4(v+1)^4(v^2+v+1)^4(v^2-v+1)^4 \end{aligned}$$

Therefore by lemma 1 we can write $D = G^2 - (At - B)$, where $\deg_t G = 2$ and $A, B \in \mathbf{Q}(v)$. Hence letting $t = B(v)/A(v)$ we get that $D$ is a perfect square in $\mathbf{Q}(v)$ and we get an eighth rational point.

In the end we check that everything fits well. The discriminant of the elliptic curve thus obtained is of degree 1296. It factors over $\mathbf{Q}[v]$ as $P(v)^4Q(v)^2$, where $P$ and $Q$ are coprime and $Q$ is irreducible of degree 468. Consequently, it is not a 12-th power in $\mathbf{C}[v]$ and hence the curve is not isomorphic over $\mathbf{Q}(v)$ to a constant curve.

If we set the point at infinity as origin, the other seven rational points are proved to be independent as is proved by specialisation (for $v = 2$ the height matrix has determinant $44435390119934.6473\ldots \neq 0$ ). Quod erat demonstrandum.

□

## 6.2 About the genus of $C$

It is natural to ask ourselves what the genus of the curve $C$ appearing in theorems 31 and 29 is. As explained in [Mes 7] it is basically 10 if $j(E) \neq j(E')$, 6 if $j(E) = j(E') \neq 0,\ 1728$ and 2 if $j(E) = j(E') = 0$ or 1728. Is it possible to find $C$ of smaller genus with the same properties?

**Theorem 33** *Let $E \ncong E'$ be two elliptic curves defined over $k$ such that at least one of them is without CM. Given a rational prime $\pi$ such that $E[\pi] \cong E'[\pi]$ inducing an anti-isomorphism for the Weil paring, then there exists a $C$ of genus 2 (notations as in theorem 31) such that $p$ and $p'$ are independent and* $\deg p = \deg p' = \pi$.

Remarks:

1. It is easy to prove the theorem in the special case when $\pi = 2$ and all the points of order 2 of $E$ and $E'$ are in $k$: let $y^2 = \prod_{i=1}^3 (x - x_i) = f(x)$ and $y^2 = \prod_{i=1}^3 (x - x_i') = g(x)$ be equations for $E$ and $E'$ respectively.

Then there exists $h \in \mathbf{PGL}_2(k)$ such that $h(x_i) = x'_i$, $i = 1, 2, 3$. By hypothesis $h(x) = (\alpha x + \beta)/(\gamma x + \delta) \not\equiv x$.

Consider now the identity

$$y^2 = g(h(x)) = \prod_{i=1}^{3}(h(x) - x'_i) = c\frac{(x - x_1)(x - x_2)(x - x_3)}{(\gamma x + \delta)^3}$$

where $c$ is a constant which can be put equal to 1. If we define the new quantities $u^2 = \gamma x + \delta$ and $Y = yu^3$ the previous equation is transformed into

$$Y^2 = \mathcal{L}(u) \tag{6.5}$$

where $\mathcal{L}$ is an even polynomial of degree 6. Let $C$ be the hyperelliptic curve of genus 2 given by 6.5. Then it is clear that the two morphisms from $C$ to (resp.) $E$ and $E'$ are given by

$$\begin{array}{rcl} (u, Y) & \longmapsto & (\frac{u^2 - \delta}{\gamma}, \frac{Y}{u^3}) \\ (u, Y) & \longmapsto & (\frac{u^2 - \delta}{\gamma}, Y) \end{array}$$

2. Let $E = E'$ be given by $y^2 = x^3 - ax + b$ and suppose that there exist $u, v \in k$ such that $a = u^2 - uv + v^2$. The conic given by $x_1^2 + x_1x_2 + x_2^2 = a$ is then $k$- isomorphic to the projective line, hence there exist two distinct rational functions of degree 2, namely $x_1(t)$ and $x_2(t)$ such that the rational function $f(t) = x_1^3 - ax_1 + b$ be equal to the rational function $x_2^3 - ax_2 + b$.

   There exist two morphisms from $C$ of equation $y^2 = f(t)$ to $E$ given by $(t, y) \mapsto (x_i(t), y)$ $(i = 1, 2)$. They are checked to be independent and, since the genus of $C$ is 3, we have in this case a curve of lower genus covering $E$.

# Chapter 7

# $p$-rank of quadratic fields

Another question related to the topics studied in the last chapter regards the $p$-rank of quadratic fields (over the rationals), i.e. the $p$-rank of their ideal class group. Let us introduce some notations.

Let $d \in \mathbf{Z}$ and $K = \mathbf{Q}(\sqrt{d})$. We call $G$ the ideal class group of $K$. By Dirichlet's theorem it is a finite abelian group, therefore it makes sense, given a prime $p$, to speak of the $p$-rank of $G$ (or $K$) as the $\mathbf{F}_p$-dimension of $G/pG$.

## 7.1 Algebraic theory

When $p = 2$, it has been known since Gauß that the 2-rank of $K$ is more or less equal to the number of prime divisors of the discriminant $\Delta$ of $K$. In particular, this rank is not bounded.

But when $p$ is an odd prime very little is known. We don't even know whether the $p$-rank is bounded! As we shall see today there is one general result, whereas all other theorems deal with specific primes (but even in those cases we don't know much). For $p = 3$ for example we have

**Theorem 34 (Craig)** *There exist infinitely many quadratic fields with* 3-*rank* $\geq 4$.

The method in treating this problem always reduces to the equation

$$y^2 = 4x^n + d \tag{7.1}$$

We give here a brief exposition of the first part of [Yam].

**Theorem 35** *Let* $(x, y) \in \mathbf{Z}^2$ *be a solution to 7.1 in coprime integers. Then*

1. *The ideal $I = (x, (y + \sqrt{d})/2)$ is of exponent $n$ in $K$.*

2. *Let $\Delta < -4$. Take a prime $p|n$ and suppose that there exists a prime $\ell$ dividing $x$ such that $y$ is a $p$-th power non-residue $\pmod{\ell}$. Then $I^n = ((y + \sqrt{d})/2)$ is not the $p$-th power of a principal ideal of $K$.*

Proof: Call $\alpha = (y + \sqrt{d})/2$. It is an integer of $K$.

1. Since $(x) \subset I$ we have taking norms
$$N(I)|N(x) = x^2 \tag{7.2}$$
Also calling $I^\sigma = (x, (y - \sqrt{d}/2))$ we readily obtain from 7.1
$$(xy) \subset II^\sigma \subset (x)$$
which implies
$$x^2|N(I)^2|(xy)^2$$
Now since $(x, y) = 1$ by hypothesis we get in view of 7.2
$$N(I)^2 = x^2$$
whence $N(I) = |x|$. Also from 7.1 we get $I^n \subset (\alpha)$, hence after taking norms $I^n = (\alpha)$.

2. Suppose there exists $a \in \mathcal{O}_K$ such that
$$(a)^p = (\alpha) \Longleftrightarrow a^p = \pm\alpha$$
since $\Delta < -4$. By juggling with Galois action and $\pm y$ we may as well suppose that $a^p = \alpha$. Now since $\ell \neq 2$ we have $\ell|x \Rightarrow y^2 \equiv d \pmod{\ell}$ and again we may suppose that
$$y \equiv \sqrt{d} \pmod{\ell} \Rightarrow \alpha \equiv y \pmod{\ell} \Rightarrow y \equiv a^p \pmod{\ell}$$
Now since $\gcd(I, I^\sigma) = 1$ and
$$II^\sigma \subset (x) \subset (\ell)$$
we obtain that $\ell$ is decomposed in $K$ so that its residue field is isomorphic to $\mathbf{F}_\ell$ and there exists therefore $b \in \mathbf{Z}$ such that $y \equiv b^p \pmod{\ell}$, contradiction.

□

This theorem has a corollary:

**Theorem 36 (Nagel, 1922)** *For any $p$, there exist infinitely many imaginary quadratic fields $K$ such that $p|h(K)$, where $h(K)$ is the class number of $K$.*

The idea of the proof is to impose on $x$ and $y$ certain congruences and to define $d = y^2 - 4x^p$. Yamamoto proves the infinity by noticing that one can also impose to a finite set $S$ of rational primes to be ramified in $K$.

The main contribution of Yamamoto is the following

**Theorem 37 (Yamamoto, 1973)** *For any $p$ there exist infinitely many imaginary $K$ of $p$-rank $\geq 2$. For any $p$ there exist infinitely many real $K$ of $p$-rank $\geq 1$.*

The idea of the proof is a modified version of theorems 35 and 36: Yamamoto takes two sets $(x, y), (x', y')$ of solutions to 7.1 and applies to each one theorem 35 but links the two solutions together by imposing that $(y + y')/2$ be a $p$-th power residue $\pmod{\ell}$. He then arrives to the conclusion. To deal with the infinity of such fields, he uses the identity

$$(u^p + v^p - w^p)^2 - 4u^pv^p = (u^p - v^p + w^p)^2 - 4u^pw^p = (u^p - v^p - w^p)^2 - 4v^pw^p$$

combined with the ideas already present in Nagel's theorem.

Let's mention two other results.

**Theorem 38 (Gross, Röhrlich)** *Let $p = 5, 7, 11$. Then if $x \in \mathbf{Q} - \{1\}$ and $1 - 4x^p < 0$ we have $p|h(1 - 4x^p)$.*

Proof: Let $d = 1 - 4x^p$. Then again as in theorem 35 $I = (x, (1 - \sqrt{d})/2)$ has order $p$. If it were trivial then there would exist $u \in K$ such that $u^p = (1 - \sqrt{d})/2$. By conjugation in $K$ also $\overline{u}^p = (1 + \sqrt{d})/2$, so that after summing $1 = u^p + \overline{u}^p$.

But Gross and Röhrlich show that there are no nontrivial point defined over $\mathbf{Q}(\sqrt{d})$ on this Fermat curve, and so we are done.

□

By the same methods they also prove

**Theorem 39** *Let $p$ be a prime greater than 3. If $x \in \mathbf{N} - \{0, 1\}$ then $p|h(1 - 4x^p)$.*

## 7.2 Geometric interpretation

### 7.2.1 General theory

There is a geometric interpretation of these facts that helps constructing a criterion to find large $p$-ranks in quadratic fields (with emphasis on real ones).

Let $E$ be an elliptic curve defined over $\mathbf{Q}$ and $R$ a rational point on $E$ of order $n$. Let $F = E/ < R >$ be the quotient curve and $\phi : E \to F$ be the corresponding isogeny. Suppose that $\phi$ is given in the simple form:

$$x \to p(x), \ y \to q(x)y \tag{7.3}$$

Take now a point $P$ in $F(K)$ (where $K$ is a number field, in our case a quadratic field). We have that $\phi^{-1}(P) = \{Q + iR, \ i = 0, \dots, n-1\}$. Now consider the field $M = K(Q)$ obtained from $K$ by adjoining the coordinates of $Q$. $M$ does not depend on $Q \in \phi^{-1}(P)$ because $R$ is rational and of the addition law on an elliptic curve. Furthermore, by 7.3 if $\alpha \in \mathbf{C}$ is such that $p(\alpha)$ is the abscissa of $P$, we have that $M = K(\alpha)$ and hence either $M = K$ or it is a cyclic extension of $K$ of degree dividing $n$ (to see it is cyclic, note that the morphism $Q \to Q+R$ when restricted to the abscissæ is a generator of the Galois group). Also we remark that $M = K$ if and only if $Q \in E(K)$.

Thus to any non-trivial point of $F(K)/\phi(E(K))$ we can attach in a natural way a non-trivial cyclic extension of $K$ of degree dividing $n$.

We can also describe everything in terms of Galois cohomology. Let $L$ be a Galois closure of $K$, $G = \mathrm{Gal}(L/K)$, then we have the exact sequence of $G$-modules:

$$0 \longrightarrow < R > \cong \mathbf{Z}/n\mathbf{Z} \longrightarrow E(L) \longrightarrow F(L) \longrightarrow 0$$

giving rise to the long cohomology sequence

$$\cdots \longrightarrow H^0(E(L)) \longrightarrow H^0(F(L)) \longrightarrow H^1(\mathbf{Z}/n\mathbf{Z}) \longrightarrow \cdots$$

Since $H^0(A)$ is by definition the submodule of $A$ consisting of elements fixed by $G$ and $G$ acts trivially on $< R >$ the previous sequence translates into

$$\cdots \longrightarrow E(K) \longrightarrow F(K) \longrightarrow \hom(G, \mathbf{Z}/n\mathbf{Z}) \longrightarrow \cdots$$

Any $\sigma \in \hom(G, \mathbf{Z}/n\mathbf{Z})$ defines a field, namely the fixed field of $\ker \sigma$. This field is Galois over $K$ with Galois group $\sigma(G) \subset \mathbf{Z}/n\mathbf{Z}$, hence cyclic.

Suppose now that $n$ is prime. We then see that $r$ independents points in $F(K)/\phi(E(K))$ give rise to $r$ independent number fields $M$, cyclic and of degree $n$ over $K$ (that is, the $\sigma$'s defining the $M$'s are independent). If $G$ is abelian, this means that its $n$-rank is at least $r$.

The link between this and $\mathrm{Cl}(K)$ is given by class field theory, which says that there is a $L$ such that $G = \mathrm{Cl}(K)$ and it is precisely the maximal unramified abelian extension of $K$ (the Hilbert class field of $K$). Hence the problem of showing that the $p$-rank of $\mathrm{Cl}(K)$ is large reduces to finding in an equally large number of independent unramified extensions of $K$ that are cyclic of degree $p$.

To study ramification, it is more convenient to introduce schemes.

Start with the curve $C$ of equation $y^2 = 4x^p + d$ and set $K = \mathbf{Q}(\sqrt{d})$. Then under the morphism $f : C \to J(C)$ sending infinity to zero we have that the point $P = (0, \sqrt{d})$ is sent to a point of $J(C)$ of order $p$ (because the divisor of $y - \sqrt{d}$ is $p(P - \infty)$). Let $A$ be the quotient variety $J(C)/ < P >$, then we have an exact sequence

$$0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow J(C) \longrightarrow A \longrightarrow 0$$

and by duality

$$0 \longrightarrow \boldsymbol{\mu}_p \longrightarrow B \longrightarrow J(C) \longrightarrow 0$$

Then there exists a group scheme $A'$ of generic fiber $J(C)$ and smooth over $\mathcal{O}_K$ giving the following exact diagram, which we get from short exact sequences (cf [Mes 6]):

$$\begin{tikzcd}
 & & 0 \arrow[d] \\
 & & \mathcal{O}_K^*/(\mathcal{O}_K^*)^p \arrow[d] \\
0 \arrow[r] & A'(\mathcal{O}_K)/B(\mathcal{O}_K) \arrow[r] & H^1(\mathrm{Spec}(\mathcal{O}_K), \boldsymbol{\mu}_p) \arrow[d] \\
 & & \mathrm{Cl}(K)_p \arrow[d] \\
 & & 0
\end{tikzcd}$$

where $\mathrm{Cl}(K)_p$ is the $p$-th component of the class group of $K$.

Now any point $(x, y) \in C(K)$ get mapped via $f$ to a point of $J(C)(K)$. The condition that $x, y$ be coprime then insures that the image of this point extends to a point of $A'(\mathcal{O}_K)$, thus giving an element of $\mathrm{Cl}(K)_p$. We therefore recover Yamamoto's application giving for coprime integers $(x, y)$ such that $y^2 = 4x^p + d$ the ideal $I = (x, (y - \sqrt{d})/2)$ of order 1 or $p$. Now in this case there is an explicit description of $B$ and the morphism $B \longrightarrow J(C)$. Indeed $B$ is a quotient of the jacobian of the Fermat curve $u^p + v^p = \sqrt{d}$. This fact enables us to understand the conditions in theorem 35 under which the ideal $I$ has exactly order $p$. Furthermore the point $(x, y)$ of $C$ has a non zero image in $A'(\mathcal{O}_K)/B(\mathcal{O}_K)$.

If $K$ is imaginary quadratic and if there exist two independent points in $A'(\mathcal{O}_K)/B(\mathcal{O}_K)$ then we can deduce the independence of the corresponding ideals of $\mathrm{Cl}(K)_p$ (note also that addition of these points on $J(C)$ corresponds to the product of the corresponding ideals).

If $K$ is real quadratic the fact that $\mathcal{O}_K^*/(\mathcal{O}_K^*)^p$ has rank one only enables us to conclude that $\mathrm{Cl}(K)_p \neq 1$. The weakness of Yamamoto's method is that it relies on the structure of the units of $K$.

We can avoid this problem by considering, instead of $H^1(\mathrm{Spec}(\mathcal{O}_K), \boldsymbol{\mu}_p)$ the group scheme $\mathbf{Z}/p\mathbf{Z}$ giving the cohomology group $H^1(\mathrm{Spec}(\mathcal{O}_K), \mathbf{Z}/p\mathbf{Z})$ $= \mathrm{hom}(\mathrm{Cl}(K), \mathbf{Z}/p\mathbf{Z})$.

Suppose now we are given an abelian variety $E$ together with a point $P$ of order $p$ and call $F = E/ < P >$. Take the Néron model of $E$ over $\mathbf{Z}$ and call it $E$ again. Suppose also that corresponding to $P$ we have a morphism $0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow E$. Then there exists a group scheme $F'$ of generic fiber $F$ such that we have the exact sequence

$$0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow E \longrightarrow F' \longrightarrow 0$$

yielding

$$0 \longrightarrow F'(\mathcal{O}_K)/E(\mathcal{O}_K) \longrightarrow \mathrm{hom}(\mathrm{Cl}(K), \mathbf{Z}/p\mathbf{Z})$$

This gives a lower bound for the $p$-rank of $K$ by the rank of $F'(\mathcal{O}_K)/E(\mathcal{O}_K)$, where the units of $K$ don't come into play anymore.

### 7.2.2 Examples

We choose $E$ to be an elliptic curve with a rational point. By Mazur's theorem $p = 3, 5, 7$. Such $E$'s are classified by the curves $X_1(p)$ which are of genus 0. Also by Vélu's formulas we can construct $F$ explicitly. For example $X_1(5)(\mathbf{Q})$ is given by the family of cubics

$$y^2 + uxy + v^2(u - v)y = x^3 + v(u - v)x^2 \qquad [u, v] \in \mathbf{P}^1(\mathbf{Q})$$

**Theorem 40 (Mestre)** *There exist infinitely many real quadratic fields with* 5*-rank (resp.* 7*-rank)* $\geq 2$.

Idea of proof: In pratice we don't need to invoke scheme theory because everything is explicit. As an example we gave Vélu's formula for $X_1(5)$, but we also know $F$ and the quotient isogeny $\phi$. Now if for some value of $[u, v]$ we can impose to $F$ to be semistable, then a sufficient condition for $K(Q)$ to be unramified over $K$ is that the point $P = \phi(Q)$ not be congruent to the node of $F$ modulo the bad primes. This amounts to imposing congruence conditions on $x \in \mathbf{Q}$ if $P = (x, \sqrt{g(x)})$ (in the scheme dictionnary this would ensure that $P$ comes from a point in the associated scheme $F'$).

Thus we already have infinitely many quadratic fields $K = \mathbf{Q}(\sqrt{g(x)})$ ($x \in \mathbf{Q}$ not in some arithmetic progression) with 5-rank $\geq 1$. By considering several values of $[u, v]$ we get $g(x)$ of arbitrary sign.

Now it is possible to construct infinitely many points $P_i = (x_i, y)$ ($i = 1, 2, 3$) on $F$ such that $x_i \in \mathbf{Q}$ and $y$ is quadratic over $\mathbf{Q}$. (This is equivalent to finding conditions so that a conic has a rational point $(x_1, x_2)$; hence we parametrize it by $t \in \mathbf{Q}$). Then after calling $K = \mathbf{Q}(y)$ we can arrange for the relative extensions $K(Q_i)$ to be unramified over $K$ (congruence condition on $t$ ). Since the $P_i$'s lie on the same line they are not independent, but we can find conditions under which two of them are (in $F(K)/\phi(E(K))$). These are congruence conditions again ($t$ belonging to some arithmetical progression). Hence the theorem is proved.

□

Remark: Let $p$ be a prime and $k \in \mathbf{N}$. Assume we can find an hyperelliptic curve over $\mathbf{Q}$ such that its Jacobian contains $(\mathbf{Z}/p\mathbf{Z})^k$ as a rational subgroup (or better $(\boldsymbol{\mu}_p)^k$). Then by a similar method we can prove that there exist infinitely many quadratic fields with $p$-rank $\geq k$.

In the same way Mestre was able to prove

**Theorem 41** *There are infinitely many real (resp. imaginary) quadratic fields of* 5*-rank* $\geq 3$ ([Mes 1])*. There are infinitely many real (resp. imaginary) quadratic fields of* 3*-rank* $\geq 5$ (unpublished).

# Chapter 8

# Hyperelliptic curves I

The last two chapters will be devoted to the study of hyperelliptic curves in an attempt to produce results similar to those on elliptic curves. Let's recall a definition.

**Theorem 42** *Let $C$ be a curve of genus $g \geq 2$ defined over a field $k$. Let $K$ be its canonical divisor. Then the following are equivalent:*

1. *There exists $f: C \to \mathbf{P}^1$ of degree 2.*

2. *There exists an involution $w: C \to C$ such that genus$(C/w) = 0$.*

3. *Let $\phi : C \to \mathbf{P}^{g-1}$ be the morphism associated to $K$. Then $\phi$ is not an embedding.*

Remark: It is known that $\deg K = 2g-2$. If $\mathcal{L}(K) = \{f \in k(C) : (f) + K \geq 0\}$ then $\mathcal{L}(K) \cup \{0\}$ is a vector space of dimension $g$ and given a basis $f_0, \ldots, f_{g-1}$ of this vector space $\phi$ is given by $x \mapsto (f_0(x), \ldots, f_{g-1}(x))$.

**Definition 5** *Any curve $C$ of genus at least 2 satisfying the equivalent conditions of the above theorem is called an hyperelliptic curve and the corresponding $w$ is called the hyperelliptic involution (see also below).*

Remark: A curve of genus 2 is always hyperelliptic because the morphism associated to $K$ gives a morphism onto $\mathbf{P}^1$ of degree 2.

Next we list a few properties of hyperelliptic curves.

**Theorem 43** 1. *The involution $w$ is unique and defined over $k$.*

2. *For any $f \in \mathrm{Aut}(C)$ we have $f \circ w = w \circ f$.*

*3. The morphism $\phi$ factors through $C/w$.*

¿From now on we assume char $k \neq 2$. The next proof is widely known but seldom found in literature.

**Theorem 44** *Let $C$ be a hyperelliptic curve of genus $g$ defined over $k$. If $g$ is even, then $C/w \cong_k \mathbf{P}^1$ (i.e. $C/w$ admits a $k$-rational point) so that $C$ admits over $k$ an hyperelliptic equation $y^2 = f(x)$ with $\deg f = 2g+2$. In these coordinates we have $w(x,y) = (x,-y)$.*

Proof: Consider the projection map $\pi : C \to C/w$. Since $K \in \mathrm{Div}_k(C)$ and $\deg K = 2g-2$ we can write $K$ in the form

$$K = \sum_i P_i + w(P_i)$$

and hence $\pi(K) = 2L$ where $\deg L = g-1$ and $L \in \mathrm{Div}_k(C/w)$. Let's show that this implies that $C/w$ has a $k$-rational point. Indeed if $K_0$ is a canonical divisor of $C/w$ we have $\deg K_0 = -2$ so that

$$L_1 = -L - \frac{g}{2}K_0$$

is of degree 1. If it is effective we are done. Otherwise by Riemann-Roch

$$l(L_1) - l(K_0 - L_1) = 1 + 0 + 1 \Longrightarrow l(L_1) = 2$$

and this implies that there exists $f \in k(C/w)$ such that $L_2 = (f) + L_1 \geq 0$. Since again $\deg L_2 = 1$ we are done.

□

## 8.1 Review on Elliptic Curves

Given an elliptic curve $E/k$ from its Weierstraß equation we can compute its relative invariants $c_4$ and $c_6$ (see formulas for example in prof. Murty's notes) and from these an absolute invariant $j$. If char $k \not| 6$ then

$$j = 12^3 \frac{c_4^3}{c_4^3 - c_6^2}$$

Also $\mathbf{A}^1$ is the moduli space of elliptic curves parametrized by $j$. That is

1. If $E, E'$ are elliptic curves over an algebraically closed field $k$, then $E \cong_k E' \Leftrightarrow j(E) = j(E')$.

2. If again $k = \overline{k}$ then $\forall j \in k$ there exists $E/k$ such that $j(E) = j$.

Remark: The last statement is true even if $k$ is not algebraically closed $(\star)$. This is particular to elliptic curves and we will see that this does not generalize to hyperelliptic curves.

Recall also that for general $k$ we have $E \cong_k E'$ if and only if there exists $u \in k^*$ such that $c_4(E) = u^4 c_4(E')$ and $c_6(E) = u^6 c_6(E')$.

## 8.2 Curves of genus 2

Recall that such curves are hyperelliptic and that they can be written as

$$y^2 = f(x) = x^6 + \cdots + a_6$$

over $\overline{k}$. By a homography sending three roots of $f$ to $0, 1, \infty$ we can transform it into

$$y^2 = x(x-1)(x-\alpha)(x-\beta)(x-\gamma)$$

Call $M_2$ the moduli space of curves of genus 2. Then by the above it is more or less parametrized by triples $(\alpha, \beta, \gamma) \in \mathbf{A}^3$ just as the elliptic curves in Legendre form are "more or less" parametrized by an affine parameter. We want to characterize $M_2$ that is to find an application

$$\varphi : \{\text{curves of genus } 2/k\} \to M_2(k)$$

such that

1. $\varphi(C) = \varphi(C') \Leftrightarrow C \cong_{\overline{k}} C'$.

2. $\forall P \in M_2(k)\ \exists C/\overline{k} :\ \varphi(C) = P$.

Note that we can have $P \in M_2(k)$ but no $C/k$ such that $\varphi(C) = P$ so $(\star)$ doesn't hold (in spite of a 1943 article of Deuring who proves $(\star)$ for both elliptic and hyperelliptic curves of genus 2!!).

## 8.3 Invariants and Covariants of Binary Forms

The theory of invariants and covariants of binary forms was propounded by Clebsch, Gordan et al. around 1880 and rediscovered in the Sixties by Dieudonné and Dixmier, among others. It has a lot of applications also to the field of hyperelliptic curves. We refer to [Cleb, Gor, CD] for details.

**Definition 6** *A binary form of degree $n$ is*

$$f(x,y)=\sum_{i=0}^{n} a_i x^i y^{n-i}$$

$\mathbf{GL}_2(K)$ acts on the space of binary forms with coefficients in $K$ in the "obvious" way. If

$$M=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \text{ and } \begin{pmatrix}x'\\ y'\end{pmatrix}=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}$$

then $f=\sum_{i=1}^{n} a'_i x'^i y'^{n-i}$ and we put

$$M\cdot f=\sum_{i=1}^{n} a'_i x^i y^{n-i}$$

Now if $f_i$ is a binary form, let $a^{(i)}$ represent its set of coefficients and $a'^{(i)}$ those of $M\cdot f$.

**Definition 7** *Let $f_1,\ldots,f_m$ be a family of binary forms.*

- *A* **covariant** *of $f_1,\ldots,f_m$ is a polynomial $C(a^{(1)},\ldots,a^{(m)},x,y)$ homogeneous in $(x,y)$ such that*

$$C(a^{(1)},\ldots,a^{(m)},x,y)=(\det M)^{-k}C(a'^{(1)},\ldots,a'^{(m)},x',y')$$

- *The* **order** *of $C$ is the total degree of $C$ in $(x,y)$.*
- *The* **degree** *of $C$ is $\deg_{(a^{(1)},\ldots,a^{(m)})}C$.*
- *The* **index** *of $C$ is $k$.*
- *$C$ is a* **(relative) invariant** *if its order is $0$.*
- *An* **absolute invariant** *is a quotient of two relative invariants of same index.*

Example: $f_i$ is a covariant of index 0.

**Theorem 45 (A property of covariants)** *Let $m = 1$ in the above definition and $C$ be a covariant of index $k$ of $f = f_1$ binary form of degree $n$. If $r$ is the degree and $l$ is the order of $C$ we have the relation*

$$k = \frac{nr - l}{2}$$

*In particular if $C$ is an invariant then $k = nr/2$.*

Remark(Transitivity of the covariant/invariant property): If $C_1, \ldots, C_r$ are covariants of $f_1, \ldots, f_m$ and $D_1, \ldots, D_s$ are covariants of $C_1, \ldots, C_r$, then they are also covariants of $f_1, \ldots, f_m$.

## 8.4 Symbolic computation

Let $\mathcal{I}_n^m$ (resp. $\mathcal{C}_n^m$) be the algebra of invariants (resp. covariants) of $m$ binary forms of degree $n$, with usual addition and multiplication. It was a major problem in the last century to determine whether these algebras are finitely generated and to find explicit generators for them. Usually one found the generators and a posteriori the algebra was finitely generated. However one proof was required for each $n, m$ and the larger the numbers, the more difficult the proof (actually, we know explicit generators only in finitely many cases, all with $n \leq 8$).

Then came Hilbert who showed in one stroke that for all $n, m$ the algebras $\mathcal{I}_n^m$ and $\mathcal{C}_n^m$ are finitely generated. His arguments involved a property of these rings called today Noetherianity. The drawback of Hilbert's theorem is that it does not produce an explicit system of generators. Therefore for computational purposes the methods of his predecessors are still valid.

To find explicit generators, we will first define a binary operator on the algebra of all covariants. If $f$ (resp. $g$) is a binary form of degree $n$ (resp.$m$) we define

$$(fg)_k = \frac{(m-k)!\,(n-k)!}{m!\,n!} \sum_{i=0}^{k} (-1)^i \left( \begin{array}{c} k \\ i \end{array} \right) \frac{\partial^k f}{\partial x^i \partial y^{k-i}} \frac{\partial^k g}{\partial y^i \partial x^{k-i}}$$

It is well-defined as we readily check and $\mathrm{ord}(fg)_k = m + n - 2k$. Moreover, if $\deg f = \alpha$ and $\deg g = \beta$ (as covariants), then $\deg(fg)_k = \alpha + \beta$.

We can combine two or more of these operators through symbolic computation, an example of which is provided by Leibniz' rule to compute derivatives of products. The trick is to deal with the operator $f \mapsto f^{(n)} = \partial^n f/\partial x^n$ as if it were the operator $f \mapsto f^n$ ( with exception $f^0 = f$). For example using this rule we have, symbolically

$$\frac{\partial^i f}{\partial x^i}\frac{\partial^j f}{\partial x^j} = \frac{\partial^{i+j} f}{\partial x^{i+j}}$$

and also

$$\frac{d^n(fg)}{dx^n} = (f+g)^{(n)}$$

Also by symbolic computation $(fg)_k(cd)_l$ is a covariant of $c, d, f, g$. It is clear that starting from invariants we obtain invariants.

## 8.5 Explicit Generators

We give without proof explicit generators of some of the algebras defined previously.

1. Let $f = ax^2 + bxy + cy^2$. Then $(ff)_1 = 0$ and $4(ff)_2 = -2(\Delta) = 2(4ac - b^2)$. We have $< f, \Delta >= \mathcal{C}_2^1$.

2. Take $f$ as before and $g = a'x^2 + b'xy + c'y^2$. Define

$$i = 2(fg)_1 = (ab' - a'b)x^2 + 2(ac' - a'c)xy + (bc' - b'c)y^2$$

   We have $(ii)_2 = -2\text{disc}(i) = -2\text{res}(f, g)$. Also $D = (ff)_2$, $D' = (fg)_2$ and $D'' = (gg)_2$ generate $\mathcal{I}_2^2$. For example

$$\begin{array}{rcl} -2i^2 & = & Df^2 - 2D'fg + D''g^2 \\ 2(if)_1 & = & Dg - D'f \\ 2(ii)_2 & = & DD'' - D'^2 \end{array}$$

3. Let $f$ be binary of degree 4. Define covariants

| *covariant* | *degree* | *order* |
|---|---|---|
| $C_4 = (ff)_2$ | 2 | 4 |
| $C_6 = (fC_4)_1$ | 3 | 6 |
| $I_2 = (ff)_4$ | 2 | 0 |
| $I_3 = (fC_4)_4$ | 3 | 0 |

Then $f$ together with the quantities defined above generate $\mathcal{C}_4^1$. We also have the important relation

$$12C_6^2 = -6C_4^3 + 3I_2C_4f^2 - 2I_3f^3 \qquad (8.1)$$

This formula applies to find rational points on quartics. Indeed the curve $C$ given by $u^2 = f(x,1)$ is a quartic. The elliptic curve $E$ of equation

$$12v^2 = -6X^3 + 3I_2X - 2I_3$$

is isomorphic to $\mathrm{Jac}(C)$. The classical covering of a quartic onto its Jacobian can therefore be given in explicit form by

$$\begin{array}{ccc} C & \longrightarrow & E \\ (x,u) & \longmapsto & (\frac{C_4}{u^2}, \frac{C_6}{u^3}) \end{array}$$

4. Let $x_1, x_2, x_3$ be three binary quadratic forms (in $x, y$). To them we can associate a conic $C$ given by the image of

$$\begin{array}{ccc} \mathbf{P}^1 & \longrightarrow & \mathbf{P}^2 \\ [x,y] & \longmapsto & [x_1(x,y), x_2(x,y), x_3(x,y)] \end{array}$$

The conic $C$ is non degenerate if the determinant $R$ of the $x_i$'s in the basis $x^2, xy, y^2$ is not zero. Define now $x_1^* = (x_2x_3)_1$, $x_2^* = (x_3x_1)_1$ and $x_3^* = (x_1x_2)_1$. The $x_i^*$ are again quadratic forms, so that we can again associate a conic $C^*$ to them. We have the fundamental relation

$$x_1x_1^* + x_2x_2^* + x_3x_3^* = 0$$

This relation tells us that if $R \neq 0$, then $C^*$ is the dual conic of $C$. The intrinsic equation of $C^*$ is of the form

$$\sum_{1 \leq i,j \leq 3} A_{ij}x_i^*x_j^* = 0$$

and one can show that $A_{ij} = (x_ix_j)_2$ (it is therefore an invariant as is to be expected). On the same lines

$$R = -(x_1x_2)_1(x_2x_3)_1(x_3x_1)_1$$

and $2R^2 = \det(A_{ij})$.

5. In general if $f$ is a binary quadratic form we have

$$Rf = (fx_1)_2 x_1^* + (fx_2)_2 x_2^* + (fx_3)_2 x_3^*$$

and if $f$ is a binary form of degree $2n$

$$R^n f = (\sum_{i=1}^{3} (fx_i)_2 x_i^*)^{(n)} = \sum_{1 \leq i_1, \ldots, i_n \leq 3} a_{i_1,\ldots,i_n} x_{i_1}^* \ldots x_{i_n}^*$$

where the $a_{\ldots}$ are invariants.

6. What is written in the previous two points can be applied to retrieve the zeros of $f$ in the projective plane. Indeed suppose $R \neq 0$ (i.e. that we take three independent quadratic forms $x_i$) and let $f$ be binary of degree $2n$. If the $x_i^*$'s are as above we found that

$$\textstyle\sum_{1 \leq i,j \leq 3} A_{ij} x_i^* x_j^* = 0 \qquad (8.2)$$

$$R^n f = \textstyle\sum_{1 \leq i_1, \ldots, i_n \leq 3} a_{i_1,\ldots,i_n} x_{i_1}^* \ldots x_{i_n}^* = 0 \qquad (8.3)$$

are the equations of a conic $C^*$ and a curve $T$ of degree $n$.

If $f = c \prod_{i=1}^{2n} (\alpha_i x - \beta_i y)$ then it is clear that the zeros of $f$ are exactly given by $C^* \cap T$.

# Chapter 9

# Hyperelliptic curves II

## 9.1 Invariants and covariants of an hyperelliptic curve

We continue to assume throughout the rest of the chapter that char $k \neq 2$. ¿From Hurwitz' formula we know that an equation

$$y^2 = f(x) = c \prod_{i=1}^{2g+2} (x - x_i)$$

where the ramification points $x_i$ are all distinct, gives an hyperelliptic curve of genus $g$. Reciprocally, any hyperelliptic curve over $k$ has an equation of this type $\underline{\text{over } \overline{k}}$ (see also theorem 44).

In general it is difficult to see if two given algebraic curves are isomorphic. However in the case of hyperelliptic curves the situation is much simpler, as we state in the following proposition.

**Proposition 1** *Given two hyperelliptic curves $C$ and $C'$ defined over a field $k$, $C$ is isomorphic to $C'$ over $\overline{k}$ (denoted $C \cong_{\overline{k}} C'$) if and only if there exists $\sigma \in \mathbf{PGL}_2(\overline{k})$ such that*

$$\sigma(\{\textit{ram. points of } C\}) = \{\textit{ram. points of } C'\}$$

In other terms, let $C$ and $C'$ be given respectively by $u^2 = f(x)$ and $U^2 = F(X)$. Call $\tilde{f}(x, y)$ and $\tilde{F}(X, Y)$ the homogenized polynomials of $f$ and $F$ (i.e. $f(x) = \tilde{f}(x, 1), \ldots$). Then it is easy to see that $C \cong_{\overline{k}} C' \Longleftrightarrow \tilde{f}(x, y)$ and $\tilde{F}(X, Y)$ are in the same orbit $\pmod{\mathbf{PGL}_2(\overline{k})}$ (cf section 8.3).

To an hyperelliptic curve of genus 2 over $k$ we can associate a sextic form $f$ with coefficients in $k$ (cf theorem 44). We then define

$$\begin{aligned} i &= (ff)_4 \\ \Delta &= (ii)_2 \\ x_1 &= (fi)_4 \\ x_2 &= (ix_1)_2 \\ x_3 &= (ix_2)_2 \\ A &= (ff)_6 \\ B &= (ii)_4 \\ C &= (i\Delta)_4 \\ D &= (x_1x_3)_2 \end{aligned}$$

The first two are quartic forms, the following three are quadratic forms (to which we associate the "dual" forms defined in section 8.5) and the last four are invariants of even degree. Clebsch showed that $A, B, C, D$ generate all invariants of even degree and that $A, B, C, D, R$ generate all invariants of $f$ (see section 8.5 for definition of $R$). Furthermore he showed the following fundamental result:

**Theorem 46** *Let $f$ and $g$ be (binary) sextic forms. Then they are isomorphic* (mod $\mathbf{PGL}_2(\overline{k})$) *if and only if there exists $u \in \overline{k}^*$ such that*

$$A = u^2A', \ B = u^4B', \ C = u^6C', \ D = u^{10}D'$$

*where the invariants $A, B, C, D$ are defined above and relative to $f$, while $A', B', C', D'$ are the same ones relative to $g$.*

Note that we have a characterization of isomorphism for hyperelliptic curves of genus 2 which does not require the computation of the roots of a polynomial.

We now return to the problem of determining the moduli space of hyperelliptic curves of genus 2.

Since $\mathcal{D} = \mathrm{disc} f$ is an invariant of degree 10 by theorem 45, it is a polynomial expression of $A, B, C, D$.

**Theorem 47 (Igusa)** *For any $A, B, C, D$ such that $\mathcal{D} \neq 0$ there exists a sextic form $f$ with these numbers as invariants.*

Suppose now $A \neq 0$ and define absolute invariants

$$\alpha = \frac{B}{A^2},\ \beta = \frac{C}{A^3},\ \gamma = \frac{D}{A^5}$$

Then $\mathcal{D}/A^5$ is an absolute invariant, equal to $\varphi(\alpha, \beta, \gamma)$. Therefore for $A \neq 0$, the moduli space of hyperelliptic curves of genus 2 is

$$\mathbf{A}^3 - \{\alpha, \beta, \gamma :\ \varphi(\alpha, \beta, \gamma) = 0\}$$

In general the situation is technically more complicated (blow-ups...) but the flavor is the same.

## 9.2 Definition over $k$

Given $(\alpha, \beta, \gamma) \in k^3$ such that $\varphi(\alpha, \beta, \gamma) \neq 0$, does there exist $C/k$ of genus 2 with invariants $\alpha, \beta, \gamma$? And if yes, how can we construct it?

Recall from the end of section 8.5 that to a sextic $f$ we can associate a conic $C^*$ and a cubic $T$. Since their coefficients are invariants, after rescaling, we may as well suppose that they are absolute invariants. Hence, since they are of even degree, they can be expressed in terms of $\alpha, \beta, \gamma$. At this point we therefore know the equations of $C^*$ and $T$.

1. Suppose $C^*(k) \neq \emptyset$. Then we may parametrize $C^*(k)$ by $[x, y] \in \mathbf{P}^1$. Replacing $x_i^*$ by $x_i^*(x, y)$ in 8.3 we obtain a homogeneous polynomial of degree 6 whose roots are those of an $f$, by our previous discussion. Clearly $f$ has coefficients in $k$ and the equation of our hyperelliptic curve is $u^2y^4 = f(x, y)$.

2. On the other hand if $C^*(k) = \emptyset$, if $k$ is perfect and the hyperelliptic curve $C$ (over $\overline{k}$) obtained from $\alpha, \beta, \gamma$ has no exceptional automorphism (meaning that $\mathrm{Aut}(C) =< w >$) [1] then $C$ is not isomorphic to a curve defined over $k$.

   Proof: Suppose that $C$ is given by

$$y^2 = f(x) \tag{9.1}$$

[1] This is mostly the case: it is clear that $\mathrm{Aut}(C)$ is finite, so that a nontrivial automorphism must be a rotation $\rho$ in the complex plane so that $\rho^6 = \mathbf{Id}$. Hence $C$ has an equation 9.1 such that $f$ is a polynomial in $x^3$ if the order of $\rho$ is 3 or $f$ is even otherwise.

with $f \in k[x]$ of degree 6. By definition $C/w \cong_{\overline{k}} \mathbf{P}^1$. Also let

$$\mathbf{P}^1 \xrightarrow{\phi} C^*$$

be a parametrization of $C^*(\overline{k})$. Hence, a priori, $\phi$ is defined over $\overline{k}$. Let $D = \sum_{i=1}^{6} P_i$ where $P_i$ $(1 \leq i \leq 6)$ are the ramification points of $C$ (i.e. the zeros of $f$). Since $f \in k[x]$ this implies $D \in \mathrm{Div}_k(C)$. Note that from what was said previously we have

$$D \overset{\phi}{\longmapsto} C^* \bigcap T$$

For $\sigma \in \mathrm{Gal}(\overline{k}/k)$ define $\phi^\sigma = \sigma \circ \phi \circ \sigma^{-1}$. Then

$$\phi^{-1} \circ \phi^\sigma(D) = D$$

and this implies $\phi^\sigma = \phi$ because there is no exceptional automorphism. Since this holds for arbitrary $\sigma$ and since $k$ is perfect, it follows that $\phi$ is defined over $k$ and therefore $C^*(k) \neq \emptyset$, contrary to our assumption.

□

Remark: In contrast to what happens in the elliptic curve case (cf remark on page 67), the relative invariants $A, B, C, D$ are not enough to determine when two curves of genus 2 are $k$-isomorphic if $k$ is not algebraically closed. As an example take $f \in k[x]$ and the two curves $C_1$ and $C_2$ given respectively by $y^2 = f(ux)$ and $y^2 = u^3 f(x)$. Then it is readily checked that $C_1$ and $C_2$ have the same $\alpha, \beta, \gamma$, but, unless $u$ is a square in $k$, $C_1 \not\cong_k C_2$.

## 9.3 Points of high order in Jac $C$

We already saw the importance of finding large groups embedded in the Jacobian of an hyperelliptic curve in connection with the study of class groups of quadratic fields. We give here a brief overview of the work of LePrévost [LeP].

**Theorem 48**

- *For any $g$ there exists an hyperelliptic curve $C/\mathbf{Q}$ of genus $g$ such that its Jacobian contains a point of order $2g^2 + 5g + 5$.*
- *For any even $g$ there exists an hyperelliptic curve $C/\mathbf{Q}(t)$ of genus $g$ such that its Jacobian contains a point of order $2g^2 + 5g + 5$.*

- *For any $g$ there exists an hyperelliptic curve $C/\mathbf{Q}(t)$ of genus $g$ such that its Jacobian contains a point of order $2g(2g+1)$.*

Remark: Note that to obtain a point of order proportional to $g$ is easy (take the point $(0,1)-\infty = P$ on $y^2 = x^{2g+1}+1$. Then $(2g+1)P = (y-1)$).

Sketch of proof: We will expose the arguments to obtain a point of order $2g^2+2g+1$ on $C/\mathbf{Q}(t)$. Set

$$\begin{aligned} 2u &= tx^g + \frac{(x-1)^g}{t} \\ 2v &= -tx^g + \frac{(x-1)^g}{t} \end{aligned}$$

and define $C/\mathbf{Q}(t)$ by

$$y^2 = u^2 - x^{g+1}(x-1)^g = v^2 - x^g(x-1)^{g+1}$$

Then $C$ is of genus $g$. Now take the functions $\phi = y - u(x)$ and $\psi = y - v(x)$. Since

$$\begin{aligned} \phi = 0 &\implies x^{g+1}(x-1)^g = 0 \\ \psi = 0 &\implies x^g(x-1)^{g+1} = 0 \end{aligned}$$

we deduce that if

$$\begin{aligned} P_0 &= (0, u(0)) \qquad P_1 = (1, u(1)) \\ Q_0 &= (0, v(0)) \qquad Q_1 = (1, v(1)) \end{aligned}$$

then

$$\begin{aligned} (\phi) &= (g+1)P_0 + gP_1 - (2g+1)P_\infty \\ (\psi) &= gQ_0 + (g+1)Q_1 - (2g+1)P_\infty \end{aligned}$$

where $P_\infty$ is the point at infinity of $C$. Also note that

$$\left.\begin{aligned} u - v &= tx^g \\ u + v &= \frac{(x-1)^g}{t} \end{aligned}\right. \implies \left.\begin{aligned} u(0) &= v(0) \\ u(1) &= -v(1) \end{aligned}\right.$$

Therefore $P_0 = Q_0$. Also

$$Q_1 + P_1 - 2P_\infty = (y^2 - \frac{t^2}{4}) \sim 0$$

implying

$$(\psi) = gP_0 + (g+1)(2P_\infty - P_1) - (2g+1)P_\infty$$

Finally, if $D_i = P_i - P_\infty$ $(i = 0, 1)$ then

$$(g+1)D_0 + gD_1 \sim 0 \quad \text{and} \quad gD_0 - (g+1)D_1 \sim 0$$

resulting in

$$((g+1)^2 + g^2)D_0 \sim 0$$

¿From this we only have that the order of $D_0$ divides $2g^2+2g+1$ but a little more work shows that it is indeed equal to $2g^2+2g+1$.

## 9.4 Periods of hyperelliptic curves

### 9.4.1 Classical theory

Let $C/\mathbf{C}$ be a curve of genus $g > 0$. It is known that the complex vector space of holomorphic differentials on $C$ has dimension $g$. Let $\omega_1, \ldots, \omega_g$ be a basis of it and let $\gamma_1, \ldots, \gamma_{2g}$ be a basis of $\mathrm{H}_1(C, \mathbf{Z}) \cong \mathbf{Z}^{2g}$. Then the complex matrix

$$(a_{ij}) = (\int_{\gamma_i} \omega_j)_{i=1,\ldots,2g}^{j=1,\ldots,g}$$

has real rank $2g$, i.e. its $2g$ rows generate a maximal discrete subgroup $\Lambda \subset \mathbf{C}^g$. We also have an embedding

$$\begin{array}{rcl} C & \hookrightarrow & \mathrm{Jac}(C) \cong \mathbf{C}^g/\Lambda \\ P & \mapsto & (\int_{P_0}^{P} \omega_1, \ldots, \int_{P_0}^{P} \omega_g) \end{array}$$

where $P_0$ is any point on $C$ (Abel-Jacobi map).

The most effective way to compute the periods of an elliptic curve is through the arithmetic-geometric mean. It is defined as follows: take $a, b$ positive real numbers and define two sequences $a_0 = a$, $b_0 = b$

$$a_{n+1} = \frac{a_n + b_n}{2} \qquad b_{n+1} = \sqrt{a_n b_n} \tag{9.2}$$

Then it is easy to prove that $\lim a_n = \lim b_n = M(a, b) < \infty$. Actually there exists an absolute constant $\kappa$ such that

$$|a_{n+1} - b_{n+1}| < \kappa |a_n - b_n|^2$$

so that the precision of the computation is quadratic, meaning that each step doubles the number of exact digits. This fact was discovered by Gauß who used this algorithm in his celestial computations.

**Theorem 49 (Gauß )**

$$\int_0^{\pi/2} \frac{dt}{\sqrt{a^2\cos^2 t + b^2 \sin^2 t}} = \frac{\pi}{2M(a,b)}$$

It was one of Gauss' "teen" discoveries and he applied this result to $a = 1, b = \sqrt{2}$.

Take now an elliptic curve $E$ of equation

$$y^2 = 4(x-e_1)(x-e_2)(x-e_3) \qquad (e_1 > e_2 > e_3) \tag{9.3}$$

Define

$$\lambda_1 = \int_{e_1}^{+\infty} \frac{dx}{y} = \int_{e_1}^{+\infty} \frac{dx}{\sqrt{4(x-e_1)(x-e_2)(x-e_3)}}$$

and

$$\lambda_2 = \int_{e_2}^{e_1} \frac{dx}{y} = \int_{e_2}^{e_1} \frac{dx}{\sqrt{-4(x-e_1)(x-e_2)(x-e_3)}}$$

Then (cf Zagier's trick in chapter 2) $\lambda_1$ is half ($y > 0$) the "real" period and $\lambda_2$ half the "imaginary" period (resp. $= a_{11}/2$ and $a_{21}/2$ in the previous matrix).

**Theorem 50** *We have that*

$$\lambda_1 = \frac{\pi}{2M(a,b)} \qquad \text{and} \qquad \lambda_2 = \frac{\pi}{2M(a,c)}$$

*where $a = \sqrt{e_1 - e_3}$, $b = \sqrt{e_1 - e_2}$ and $c = \sqrt{e_2 - e_3}$.*

Proof: We prove only the formula for $\lambda_1$. Define a ladder of elliptic curves $a_0 = a$, $b_0 = b$ as in theorem,

$$E_n : \ y^2 = 4x(x + a_n^2)(x + b_n^2) \qquad (n \geq 0)$$

where the sequences $(a_n)$ and $(b_n)$ are those appearing in 9.2. Clearly $E_0 \cong E$ and $\lambda_1$ stays the same. Now let $\lambda_2 = a_{21}$. Then we have the following commuting ladder of morphisms, the horizontal ones being complex isomorphisms, the right vertical ones being the "natural" morphisms.

$$\begin{tikzcd}
\vdots & \vdots \\
E_n \arrow[r, "\cong"] \arrow[d] & \mathbf{C}/ < \lambda_1, 2^n\lambda_2 > \arrow[d] \\
\vdots & \vdots \\
E_1 \arrow[r, "\cong"] \arrow[d] & \mathbf{C}/ < \lambda_1, 2\lambda_2 > \arrow[d] \\
E_0 \arrow[r, "\cong"] & \mathbf{C}/ < \lambda_1, \lambda_2 >
\end{tikzcd}$$

Note that the left morphism is given by

$$x \longmapsto \frac{x(x+b_n^2)}{x+a_n^2}$$

at the $n$-th level. Therefore since $\lambda_1$ remains the same throughout the ladder we have

$$\lambda_1 = \int_0^{+\infty} \frac{dx}{\sqrt{4x(x+a_n^2)(x+b_n^2)}}$$

and hence passing to the limit

$$\lambda_1 = \int_0^{+\infty} \frac{dx}{\sqrt{4x(x+M^2(a,b))^2}} = \int_0^{+\infty} \frac{dx}{2(x+M^2(a,b))\sqrt{x}} = \frac{\pi}{2M(a,b)}$$

□

Remark: Of course there is also a purely algebraic proof. One can use for example the change of variables:

$$x = e_3 + (e_2 - e_3)\sin^2 t$$

which yields

$$4\int_{e_3}^{e_2} \frac{dx}{\sqrt{4(x-e_1)(x-e_2)(x-e_3)}} = \int_0^{2\pi} \frac{dt}{\sqrt{(e_1-e_3)\cos^2 t + (e_1-e_2)\sin^2 t}}$$

### 9.4.2 The case of hyperelliptic curves of genus 2

Take four different positive real numbers

$$a = a_0 > b = b_0 > c = c_0 > d = d_0$$

and define

$$\begin{aligned} a_{n+1} &= \frac{a_n + b_n + c_n + d_n}{4} \\ b_{n+1} &= \frac{\sqrt{a_n b_n} + \sqrt{c_n d_n}}{2} \\ c_{n+1} &= \frac{\sqrt{a_n c_n} + \sqrt{b_n d_n}}{2} \\ d_{n+1} &= \frac{\sqrt{a_n d_n} + \sqrt{c_n b_n}}{2} \end{aligned}$$

Then as before we can prove that

$$\lim a_n = \lim b_n = \lim c_n = \lim d_n = M(a,b,c,d) < \infty$$

called the Borchardt mean.

Let $C$ be an hyperelliptic curve of genus two given by

$$y^2 = (x - e_1) \cdots (x - e_6) \qquad (e_1 > e_2 > \ldots > e_6)$$

and define

$$\begin{aligned} a &= \sqrt{(e_1 - e_3)(e_1 - e_5)(e_3 - e_5)(e_2 - e_4)(e_2 - e_6)(e_4 - e_6)} \\ b &= \sqrt{(e_1 - e_4)(e_1 - e_6)(e_4 - e_6)(e_2 - e_3)(e_2 - e_5)(e_3 - e_5)} \\ c &= \sqrt{(e_1 - e_4)(e_1 - e_5)(e_4 - e_5)(e_2 - e_3)(e_2 - e_6)(e_3 - e_6)} \\ d &= \sqrt{(e_1 - e_3)(e_1 - e_6)(e_3 - e_6)(e_2 - e_4)(e_2 - e_5)(e_4 - e_5)} \end{aligned}$$

**Theorem 51** *Under previous notations we have*

$$\det \Lambda_{\mathbf{R}} = \frac{4\pi^2}{M(a,b,c,d)}$$

*where $\Lambda_{\mathbf{R}}$ is the $2 \times 2$ matrix with the real periods of $C$ as entries.*

Can we get more? We can try and build a ladder as in the case of elliptic curves. But there is a difficulty. At each step of the ladder we don't have morphisms but correspondences between $C$ and $C'$. Recall that a $(n, m)$ correspondence between $C$ and $C'$ is just an algebraic curve $\Gamma \subset C \times C'$ such that the projections $\Gamma \to C, C'$ are of degree $n$ and $m$.

$$\begin{tikzcd} C \arrow[r] \arrow[d, leftrightarrow] & \mathrm{Jac}(C) \arrow[d] \\ C' \arrow[r] & \mathrm{Jac}(C') \end{tikzcd}$$

Take the ramification points $P_1, \ldots, P_6$ of $C$. Consider them in $\mathbf{P}^1(\mathbf{R}) \cong \mathrm{S}^1$. We want to give a geometric construction of $C'$. Construct the triangle $T$ whose sides are supported by $(P_1P_2)$, $(P_3P_4)$ and $(P_5P_6)$. If we draw from its vertices the tangents to $\mathrm{S}^1$ we will get six new points on the circle, namely $P_1^1, \ldots, P_6^1$. Then $C'$ is the curve of genus two with these points as ramification points. The correspondence is easily seen to be $(2, 2)$. We can proceed inductively. We remark that, in the same way as the limit curve in the elliptic curve case is a singular cubic (therefore a rational curve), for genus 2 the six points converge to three points by pairs so that the limit curve is a union of two rational cubics.

The algebraic formulas to find $C'$ make use of invariants. Write an equation for $C$ in the form

$$y^2 = p(x)q(x)r(x)$$

where $p, q, r$ are each of degree 2. Define

$$\begin{aligned} u &= q'r - qr' &&= [q, r] \\ v &= r'p - rp' &&= [r, p] \\ w &= p'q - pq' &&= [p, q] \end{aligned}$$

Note that $u(x) = (qr)_1(x, 1)$ etc. in the notation of chapter 8. Then $C'$ is given by

$$\Delta y'^2 = u(x')v(x')w(x')$$

where $\Delta$ is the determinant of $p, q, r$ in the basis $1, x, x^2$. Also the correspondence is given by

$$\begin{cases} p(x)u(x') + q(x)v(x') = 0 \\ yy' = p(x)u(x')(x - x') \end{cases}$$

We can compute periods of curves of genus 2 by using these formulas. Indeed we need to compute integrals of the form

$$\int_a^{a'} \frac{s(x)dx}{\sqrt{|p(x)q(x)r(x)|}}$$

where $s$ is of degree at most 1, $p, q, r$ are real polynomials of degree at most 2 such that $\deg pqr = 5$ or 6 and $a, a'$ are two consecutive zeros of $p, q, r$.

Suppose that the zeros of $p, q, r$, resp. $a < a' < b < b' < c < c'$ are real and arranged in increasing order. We can then define the six sequences $(a_n), (a_n^{'}), (b_n), (b_n^{'}), (c_n), (c_n^{'})$ recursively by

- $a_0 = a, a_0^{'} = a', b_0 = b, b_0^{'} = b', c_0 = c, c_0^{'} = c'$.
- $a_{n+1} < a_{n+1}^{'} < b_{n+1} < b_{n+1}^{'} < c_{n+1} < c_{n+1}^{'}$
- $a_{n+1}, \ldots, c_{n+1}^{'}$ are the roots of $[p_n q_n][q_n r_n][r_n p_n]$ with $p_n = (x-a_n)(x-a_n^{'})$ etc. (note that $p_1 \neq u$; we are reordering the roots of $uvw$ altogether).

Now from the discussion about the limit curve, we see that there exist $\alpha < \beta < \gamma$ such that

$$\begin{aligned} \alpha &= \lim a_n &= \lim a_n^{'} \\ \beta &= \lim b_n &= \lim b_n^{'} \\ \gamma &= \lim c_n &= \lim c_n^{'} \end{aligned}$$

Using the algebraic definition of the correspondence it is not difficult to see that if $\Delta_n$ is the discriminant of $p_n, q_n, r_n$ with respect to the basis $1, x, x^2$ and if

$$t_n = 2\frac{\sqrt{\Delta_n}}{\sqrt{(b_n + b_n^{'} - a_n - a_n^{'})(c_n + c_n^{'} - b_n - b_n^{'})(c_n + c_n^{'} - a_n - a_n^{'})}}$$

then we have

$$\int_{a_n}^{a_n^{'}} \frac{s(x)dx}{\sqrt{-p_n q_n r_n(x)}} = t_n \int_{a_{n+1}}^{a_{n+1}^{'}} \frac{s(x)dx}{\sqrt{-p_{n+1}q_{n+1}r_{n+1}(x)}}$$

Therefore after setting

$$I_a = \int_a^{a'} \frac{s(x)dx}{\sqrt{-(x-a)(x-a')(x-b)(x-b')(x-c)(x-c')}}$$

and passing to the limit we obtain

$$I_a = \pi T \frac{s(\alpha)}{(\beta-\alpha)(\gamma-\alpha)}$$

where $T = \prod_{k=0}^{\infty} t_k$.

In the same way

$$\begin{aligned} I_b &= \int_b^{b'} \frac{s(x)dx}{\sqrt{-(x-a)(x-a')(x-b)(x-b')(x-c)(x-c')}} \\ &= \pi T \frac{s(\beta)}{(\beta-\alpha)(\gamma-\beta)} \end{aligned}$$

$$\begin{aligned} I_c &= \int_c^{c'} \frac{s(x)dx}{\sqrt{-(x-a)(x-a')(x-b)(x-b')(x-c)(x-c')}} \\ &= \pi T \frac{s(\gamma)}{(\gamma-\alpha)(\gamma-\beta)} \end{aligned}$$

The reader can refer to [BM] for computational details.

We conclude this topic by mentioning that there is a geometrical interpretation of the formulas given above, as was already mentioned in the explanation of Richelot's correspondence. The sequence of correspondences gives rise to a tower of (2,2)-isogenies between the jacobians of the curves $C_n$ of equation $T_{n-1}^2 y^2 = p_n q_n r_n(x)$ where $T_{n-1} = \prod_{k=0}^{n-1} t_k$. The limit curve has equation $T^2 y^2 = (x-\alpha)^2(x-\beta)^2(x-\gamma)^2$, therefore consisting of two rational components on which we are integrating our differential form $s(x)dx/y$.

# Bibliography

[BM] Jean-Benoît Bost et Jean-François Mestre *Moyenne arithmético-géométrique et périodes des courbes de genre* 1 *et* 2, Gaz. Math. no 38 (1988), p. 36–64.

[CD] James B. Carrell and Jean Alexandre Dieudonné *Invariant theory, old and new*, New York, Academic Press (1971).

[Cleb] Alfred Clebsch *Theorie der binaren algebraischen Formen*, Leipzig, B.G. Teubner (1872).

[Di] Leonard Eugene Dickson *History of the theory of numbers*, no 2, Chelsea (1971).

[Elk] Noam Elkies *Curves with many points*, preprint.

[Ferm 1] Stéfane Fermigier *Un exemple de courbe elliptique définie sur* $\mathbf{Q}$ *de rang* $\geq 19$, C.R. Acad. Sci. Paris, t.315 (1992), série I, p. 719–722.

[Ferm 2] Stéfane Fermigier *Zéros des fonctions L de courbes elliptiques*, Experiment. Math. 1 (1992), no 2, p. 167–173.

[Gor] Paul Gordan *Dr Paul Gordan's Vorlesungen über Invariantentheorie*, Leipzig, B.G. Teubner (1885-1887).

[KK] W. Keller et L. Kulesz *Courbes algébriques de genre* 2 *et* 3 *possédant de nombreux points rationnels*, C.R. Acad. Sci. Paris, t. 321 (1995), Série I, p. 1469–1472.

[KN] Tomonori Kouva and Koh-ichi Nagao *An example of an elliptic curve over* $\mathbf{Q}$ *with rank* $\geq 21$, Proc. Japan Acad. 70 (1994), p. 104–105.

[LeP] Franck LePrévost *Torsion sur des familles de courbes de genre $g$*, Manuscripta math. 75 (1992), no 3, p. 303–326.

[Mer] Loïc Merel *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Inv. Math. no. 124 (1996), p. 437–449.

[Mes 1] Jean-François Mestre *Corps quadratiques dont le* 5*-rang du groupe de classes est* $\geq 3$, C.R. Acad. Sci. Paris, t.315 (1992) no 4, série I, p.371–374.

[Mes 2] Jean-François Mestre *Courbes elliptiques de rang* $\geq 11$ *sur* $\mathbf{Q}(t)$, C.R. Acad. Sci. Paris, t.313 (1991), série I, p. 139–142.

[Mes 3] Jean-François Mestre *Courbes elliptiques de rang* $\geq 12$ *sur* $\mathbf{Q}(t)$, C.R. Acad. Sci. Paris, t.313 (1991), série I, p. 171–174.

[Mes 4] Jean-François Mestre *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, Séminaire de théorie des nombres 1979–1980, Exp. no 15, 18 pp., Univ. Bordeaux I, Talence (1980).

[Mes 5] Jean-François Mestre *Formules explicites et minorations de conducteurs de variétés algébriques*, Comp. Math. 58 (1986) p. 209–232.

[Mes 6] Jean-François Mestre *Groupes de classes d'idéaux non cycliques de corps de nombres*, Séminaire de théorie des nombres de Paris 1981–1982, p. 189–200, Progr. Math. 38, Birkhäuser, Boston, Mass. (1983).

[Mes 7] Jean-François Mestre *Rang de courbes elliptiques d'invariant donné*, C.R. Acad. Sci. Paris, t. 314 (1992), série I, p.919–922.

[Nag 1] Koh-ichi Nagao *An example of an elliptic curve over* $\mathbf{Q}(t)$ *with rank* $\geq 13$, Proc. Japan Acad. 70 (1994), p. 152–153.

[Nag 2] Koh-ichi Nagao *An example of an elliptic curve over* $\mathbf{Q}(t)$ *with rank* $\geq 20$, Proc. Japan Acad. 69 (1993), p. 291–293.

[Ser] Jean-Pierre Serre *Cours d'arithmétique*, Presses Universitaires de France (1970).

[Shio 1] Tetsuji Shioda *An infinite family of elliptic curves over* $\mathbf{Q}$ *with large rank via Néron's method*, Inv. Math. 106 (1991) p. 106–119.

[Shio 2] Tetsuji Shioda *On the Mordell-Weil lattices*, Commentarii math. Univ. Sancti Pauli, vol. 39 no. 2 (1990) p. 211–240.

[Silv] Joseph Silverman *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer Verlag (1986).

[Yam] Yoshihiko Yamamoto *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. 7 (1970) p.57–76.