UNIVERSITÀ DEGLI STUDI DI UDINE

Dipartimento di Matematica e Informatica

Dottorato di ricerca in Matematica e Fisica

XIX ciclo

Tesi di dottorato

A lower bound for the r-order of a matrix modulo N and applications to elliptic curves

Supervisore:
Prof. UMBERTO ZANNIER

Dottorando:
CARLO MAGAGNA

5 Maggio 2007

Introduction

In [3] it is shown that, if a and b are multiplicatively independent integers greater than 1, then for every positive ϵ,

$$\gcd\left(a^n - 1, b^n - 1\right) < \exp(\epsilon n),$$

for every n sufficiently large. No elementary proof of this bound is known and the proof relies strongly on Schmidt's subspace theorem (see [1, chapter 7]). This result, combined with the arguments presented in [5], can be sharpened as follows: let $\epsilon > 0$ and let S be a finite set of primes in $\mathbb{Z}$; then for u and v multiplicatively independent S-units in $\mathbb{Z}$, we have ([5, remark 1])

$$\gcd\left(u - 1, v - 1\right) \ll_{\epsilon,S} \max\left(|u|, |v|\right)^{\epsilon}. \tag{1}$$

This last result is then used in [4] to tackle the following problem: let A be a $d \times d$ non singular integer matrix and let $N \geq 1$ be an integer; the order of A modulo N, denoted $\mathrm{ord}(A, N)$, is defined to be the least positive integer k such that

$$A^k \equiv I \pmod{N}.$$

If A is not invertible modulo N, then we define $\mathrm{ord}(A, N) = \infty$. It is then interesting to study the behaviour, i.e. the minimal growth, of $\mathrm{ord}(A, N)$ as N approaches infinity. The result achieved in [4] says that

$$\lim_{N \to +\infty} \frac{\mathrm{ord}(A, N)}{\log N} = +\infty \tag{2}$$

if and only if none of the following conditions holds:

(i) A is diagonalizable and a power of A has all the eigenvalues equal to powers of a single rational integer.

(ii) A is diagonalizable and a power of A has all the eigenvalues equal to powers of a single unit in a real quadratic field.

In this thesis we will generalize this result in the following sense. Let A be a $d \times d$ non singular integer matrix and let $N \geq 1$ be an integer. We define the N-rank of A as the greatest positive integer r such that there exists an $r \times r$ minor of A whose determinant is not divisible by N. If r is such an integer, we will write $r = N\text{-rank}(A)$. If all the determinants of order 1 are divisible by N, we will say that A has N-rank 0. We then define the r-order of A modulo N to be the smallest positive integer k such that $N\text{-rank}(A^k - I) \leq r$ and we will write $k = \text{ord}(A, N, r)$. We will then study the minimal growth of $\text{ord}(A, N, r)$, for fixed values of r and given A, as N approaches ∞. For a fixed r, We will say that A is r-regular if

$$\lim_{N \to +\infty} \frac{\text{ord}(A, N, r)}{\log N} = +\infty \tag{3}$$

and that A is r-exceptional otherwise. We will then establish a necessary and sufficient condition for being r-regular. We will show that a given A is r-regular if and only if for every eigenvalue λ which is not a root of unity, the sum of the dimensions of the eigenspaces relative to eigenvalues which are multiplicatively dependent with λ and are not roots of unity, plus the dimensions of the eigenspaces relative to eigenvalues which are roots of unity, does not exceed $d - r - 1$. Our result generalizes (2), which can be recovered in the case $r = 0$. The main tools we will use in the proof are the above mentioned result (1) by Corvaja and Zannier and Roth's diophantine approximation theorem.

For certain applications it reveals to be more convenient to consider, more generally than an integer matrix, an endomorphism ϕ of a finitely generated free module over a ring of characteristic zero, without choosing a base. If all the coefficients of the characteristic polynomial of ϕ are rational integers, then such are the coefficients of the characteristic polynomial of $\phi^n - I$, for every positive integer n, where I is the identity endomorphism. We will then study the minimal growth, as $N \in \mathbb{N}$ approaches infinity, of the smallest positive integer k such that all the coefficients, suitably weighted for homogeneity, of the characteristic polynomial of $\phi^k - I$ are divisible by N.

The second part of the thesis will be of arithmetic geometry nature, and will be dedicated to apply these diophantine approximation results to study the group of rational points of elliptic curves over extensions of finite fields. As an intermediate step we will recover the following result by Luca and Shparlinski [13], providing an alternative proof. Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and let $l(q^n)$ be the exponent of the group $E\left(\mathbb{F}_{q^n}\right)$; then for every positive ϵ,

$$l(q^n) \geq q^{n(1-\epsilon)} \quad \text{for every } n \text{ sufficiently large}$$

if and only if E is ordinary (i.e. not supersingular). This amounts to say, in view of the Hasse-Weil relation for the number of rational points, that the group $E\left(\mathbb{F}_{q^n}\right)$ is

almost cyclic, when n approaches infinity, if and only if E is ordinary.
We will then extend this result to a product of two elliptic curves. If E_1, E_2 are two ordinary elliptic curves over $\mathbb{F}_q$ and if $\mathcal{A} = E_1 \times E_2$ is their product, we will show that, for every positive ϵ, the exponent $l(q^n)$ of the group $\mathcal{A}\left(\mathbb{F}_{q^n}\right)$ satisfies

$$l(q^n) \geq q^{2n(1-\epsilon)} \quad \text{for every } n \text{ sufficiently large.}$$

From this we will deduce that if E_1 and E_2 are not isogenous over an algebraic closure of $\mathbb{F}_q$, then, for every positive ϵ,

$$\gcd\left(\sharp E_1\left(\mathbb{F}_{q^n}\right), \sharp E_2\left(\mathbb{F}_{q^n}\right)\right) < \exp(\epsilon n)$$

for every n sufficiently large. This can be interpreted as an isogeny criterion for ordinary elliptic curves over finite fields: if the orders of the groups of $\mathbb{F}_{q^n}$-rational points have too many common factors as n tends to infinity, then the two curves must be isogenous. On the other hand if the two curves are isogenous, then for every n, they have the same number of $\mathbb{F}_{q^n}$-rational points.

Acknowledgments

I would like to thank prof. Umberto Zannier for suggesting me this work and for his helpful advice. I would like also to thank prof. Pietro Corvaja for the many useful discussions. I express my thanks to prof. Emmanuel Kowalski and prof. Zeev Rudnick for reading this thesis and for their remarks and hints.

Contents

Chapter 1

Diophantine approximation

1.1 A brief history of diophantine approximation

The main problem of diophantine approximation has its origins in the following question: given a real number α, how close to α can we find a rational number p/q? That is to say, given $\alpha \in \mathbb{R}$, how small can we make the difference

$$\left|\alpha - \frac{p}{q}\right| \tag{1.1}$$

by choosing $p/q \in \mathbb{Q}$? Of course, if we do not impose any restriction on p and q, then (1.1) can be made arbitrarily small, by choosing large values for p and q.
More interesting is the problem of approximating $\alpha \in \mathbb{R}$ with a rational number p/q when we set some restrictions on the possible values of p and q, in particular we would like to find good approximations with small values of p and q. More precisely we can ask, for given $\alpha \in \mathbb{R}$ and $k > 0$, if there exist or not infinitely many $p/q \in \mathbb{Q}$ such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^k} \, ? \tag{1.2}$$

The following theorem by Dirichlet, whose proof can be found in [14, chapter 1], implies that for $k = 2$ there exist infinitely many rational solutions to (1.2):

Theorem 1.1 (Dirichlet, 1842)**.** *Let $\alpha, Q \in \mathbb{R}$ and let $Q > 1$. There exist then $p, q \in \mathbb{Z}$ such that $1 \leq q < Q$ and*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}. \tag{1.3}$$

and hence

Corollary 1.2. *Let $\alpha \in \mathbb{R}$ be an irrational number. There exist then infinitely many $(p, q) \in \mathbb{Z}^2$, with p, q coprime, such that*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}. \tag{1.4}$$

On the other side one can study what happens if we strenghten the exponent $k = 2$, i.e. if we still have infinite rational solutions to (1.2), for $k > 2$. A partial answer to this problem was found by Liouville, when α is an algebraic number (see [14] for a proof):

Theorem 1.3 (Liouville, 1844)**.** *Let $\alpha \in \mathbb{R}$ be an algebraic number of degree d. Then for every $\epsilon > 0$ the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\epsilon}} \tag{1.5}$$

has only finitely many solutions.

This result was used by Liouville himself to prove the existence of transcendental numbers. An improvement of Lioville's theorem was then established by Thue by proving the following theorem.

Theorem 1.4 (Thue, 1909)**.** *Let $\alpha \in \mathbb{R}$ be an algebraic number of degree d. Then for every $\epsilon > 0$ the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{\frac{d}{2}+1+\epsilon}} \tag{1.6}$$

has only finitely many solutions.

Then Siegel made a further improvement by replacing the exponent $d/2 + 1 + \epsilon$ in Thue's theorem, with $2\sqrt{d}$. Then many other smaller exponents were found by Dyson, Gelfond and others. All this improvements had profound implications in the theory of diophantine equations, since Liouville's theorem is not strong enough in many cases (e.g. to prove that the equation $x^d - 2y^d = m$, with $m \in \mathbb{Z}$ and $d \geq 3$, has finitely many integer solutions, one needs a stronger exponent than Liouville's one).
A definitive answer was then given by Roth in 1955, by dropping any dependence of the exponent on the algebraic degree of α:

Theorem 1.5 (Roth, 1955)**.** *Let $\alpha \in \mathbb{R}$ be an algebraic number of degree $d \geq 2$. Then for every $\epsilon > 0$ the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\epsilon}} \tag{1.7}$$

has only finitely many solutions.

This result is the best possible, by Dirichlet theorem 1.1, in the sense that the exponent $2 + \epsilon$ can not be further improved. The proof of Roth's theorem is quite intricate, uses many combinatoric lemmas and can be found in [14].
To extend these results in the framework of number fields, we need to recall some basic concepts in the following section.

1.2 Places and heights

An *absolute value* on a field $\mathbb{K}$ is a function

$$|\cdot| : \mathbb{K} \longrightarrow \mathbb{R}$$

such that

(i) $|x| > 0$ for every $x \in \mathbb{K}^*$ and $|0| = 0$.

(ii) $|xy| = |x| \cdot |y|$, for every $x, y \in \mathbb{K}$.

(iii) $|x + y| \leq |x| + |y|$, for every $x, y \in \mathbb{K}$.

If the property (iii) is replaced by the stronger

(iii') $|x + y| \leq \max\{|x|, |y|\}$

then the absolute value is said *non archimedean*.
In $\mathbb{Q}$ the only archimedean absolute value $|\cdot|_\infty$ is the restriction of the usual absolute value on $\mathbb{R}$. Further, for every prime $p \in \mathbb{Z}$, we can define a non archimedean absolute $|\cdot|_p$ value as follows. For every $x \in \mathbb{Q}$, let $\mathrm{ord}_p(x)$ be the unique integer such that

$$x = p^{\mathrm{ord}_p(x)} \frac{a}{b}$$

for suitable $a, b \in \mathbb{Z}$ such that $p \nmid ab$. Then the p-adic absolute value of x is defined as

$$|x|_p = p^{-\mathrm{ord}_p(x)}.$$

The restriction of the standard absolute value on $\mathbb{R}$ and the p-adic absolute values exhaust the possible non equivalent absolute values on $\mathbb{Q}$, where *equivalent* means giving the same topology. If we denote the set of all absolute values on $\mathbb{Q}$ by $M_\mathbb{Q}$, then

$$\prod_{\mu \in M_\mathbb{Q}} |x|_\mu = 1, \quad \forall x \in \mathbb{Q}^* \quad \text{(product formula)} \tag{1.8}$$

holds, because of the unique factorization of $\mathbb{Z}$.
More generally, on a field $\mathbb{K}$, an absolute value $|\cdot|$ defines a metric in the obvious

way, and both the additive and the multiplicative group of $\mathbb{K}$ become topological groups, i.e. $\mathbb{K}$ becomes a topological field. Two absolute values are said to be equivalent if they define the same topology, and an equivalence class of absolute values is called a *place*. We will denote by $M_{\mathbb{K}}$ the set of all places of the field $\mathbb{K}$. Similarly we will denote by $M_{\mathbb{K},\infty}$ or M_∞ the set of archimedean places of $\mathbb{K}$ and by $M_{\mathbb{K},0}$ or M_0 the set of non archimedean places of $\mathbb{K}$. Archimedean and non archimedean places are often referred to as infinite and finite places respectively. For a finite set S of $M_{\mathbb{K}}$, which includes $M_{\mathbb{K},\infty}$, we define the ring of S-integers of $\mathbb{K}$ as

$$O_{\mathbb{K},S} = \left\{ x \in \mathbb{K} \mid |x|_\mu \leq 1, \forall \mu \notin S \right\}$$

and denote by $O^*_{\mathbb{K},S}$ the group of S-units of $\mathbb{K}$, i.e. the group of the invertible elements of $O_{\mathbb{K},S}$:

$$O^*_{\mathbb{K},S} = \left\{ x \in \mathbb{K} \mid |x|_\mu = 1, \forall \mu \notin S \right\}.$$

A suitable normalization of absolute values leads, as in (1.8), to the product formula

$$\prod_{\mu \in M_{\mathbb{K}}} |x|_\mu = 1, \quad \forall x \in \mathbb{K}^* \text{ (product formula).} \tag{1.9}$$

In the following we will continue to denote the set of normalized absolute values by $|\cdot|$.

To conclude this section we briefly recall the notion of height on a projective space.

Definition 1.6. Let $\mathbb{K}$ be a number field and let $\mathbb{P}_n(\mathbb{K})$ be the n-dimensional projective space over the field $\mathbb{K}$. The *absolute logarithmic Weil height* $h(P)$ of a point $P = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}_n(\mathbb{K})$ is defined as

$$h(P) = \sum_{\mu \in M_{\mathbb{K}}} \max_i \log |x_i|_\mu \,.$$

The absolute logarithmic Weil height is independent from the choice of the homogeneous coordinates and is even independent from the choice of the field $\mathbb{K}$, whom the coordinates belong to and this is why we call it *absolute*. In the following we will also use often the *multiplicative height*, or simply height, $H(P)$ of a point $P \in \mathbb{P}_n(\mathbb{K})$, which is defined as

$$H(P) = \exp(h(P)).$$

Similarly we can define the logarithmic and multiplicative height for a point P in the affine space. Let $\mathbb{K}$ be a number field, as before, and let $P = (x_1, x_2, \ldots, x_n) \in$

$\mathbb{A}^n(\mathbb{K})$. As usually we can embed the affine space in a projective space of the same dimension by the map

$$\begin{aligned} \phi : \mathbb{A}^n(\mathbb{K}) &\longrightarrow \mathbb{P}_n(\mathbb{K}) \\ (x_1, x_2, \ldots, x_n) &\longmapsto (1 : x_1 : x_2 : \ldots : x_n). \end{aligned}$$

The absolute logarithmic Weil height of P is defined as

$$h\left(\phi(P)\right)$$

and we will continue to denote it by $h(P)$, since the meaning will be clear from the context. The height of P will be of course $\exp(h(\phi(P)))$ and we will continue to denote it by $H(P)$.
For later convenience we introduce the function

$$\log^-(x) = -\min\{0, \log(x)\}.$$

Then for a point $P = x \in \mathbb{A}^1(\mathbb{K})$,

$$\begin{aligned} h(P) &= \sum_{\mu \in M_{\mathbb{K}}} \max\left\{\log(1), \log|x|_\mu\right\} = \sum_{\mu \in M_{\mathbb{K}}} \log\max\left\{1, |x|_\mu\right\} \\ &= \log \prod_{\mu \in M_{\mathbb{K}}} \max\left\{1, |x|_\mu\right\} = \log \prod_{\mu \in M_{\mathbb{K}}} \frac{1}{|x|_\mu} \max\left\{1, |x|_\mu\right\} \end{aligned}$$

where the last equality follows from the product formula (1.9). Moreover

$$\begin{aligned} \log \prod_{\mu \in M_{\mathbb{K}}} \frac{1}{|x|_\mu} \max\left\{1, |x|_\mu\right\} &= \log \prod_{\mu \in M_{\mathbb{K}}} \max\left\{1, \frac{1}{|x|_\mu}\right\} = \sum_{\mu \in M_{\mathbb{K}}} \log\max\left\{1, \frac{1}{|x|_\mu}\right\} \\ &= \sum_{\mu \in M_{\mathbb{K}}} -\log\min\left\{1, |x|_\mu\right\} = \sum_{\mu \in M_{\mathbb{K}}} -\min\left\{0, \log|x|_\mu\right\} = \sum_{\mu \in M_{\mathbb{K}}} \log^-(x) \end{aligned}$$

To summarize

$$h(x) = \sum_{\mu \in M_{\mathbb{K}}} \log^-(x). \tag{1.10}$$

This equivalent expression for the logarithmic height will be essential in chapter 3.

1.3 Diophantine approximation on number fields

In this section we present a brief overview of how diophantine approximation of section 1.1 can be extended to number fields. For more details we refer the reader to [1, chapters 6, 7] or [17, chapters I, II]. Let now $\mathbb{K}$ be a number field and let

us denote by $|\cdot|_\mu$ the absolute values of $\mathbb{K}$, normalized as explained in the previous section in a way that the product formula (1.9) holds. Moreover let us use the same notation for the extensions of the absolute values to an algebraic closure of $\mathbb{K}$. The following generalization of Roth's theorem 1.5 is due to Lang, after preliminary work by Ridout.

Theorem 1.7 (Lang, 1962)**.** *Let $\mathbb{K}$ be a number field and S a finite set of places. For each $\mu \in S$ let α_μ be $\mathbb{K}-$algebraic. Then for each $\epsilon > 0$, there exist only finitely many $\beta \in \mathbb{K}$ such that*

$$\prod_{\mu \in S} \min\left(1, |\beta - \alpha_\mu|_\mu\right) \leq H(\beta)^{-2-\epsilon}$$

Roth's theorem 1.5 can be recovered in the case $\mathbb{K} = \mathbb{Q}$ and $S = M_{\mathbb{Q},\infty}$. The theorem holds even if we allow $\alpha_\mu = \infty$, if we define $|\beta - \infty|_\mu$ to be $|1/\beta|_\mu$. As an application of theorem 1.7, one can prove the following theorem, which is due to Mahler and is a generalization of finiteness results for Thue's equations.

Theorem 1.8 (Mahler)**.** *Let $f \in \mathbb{K}[X, Y]$ be a homogeneous polynomial of degree $d \geq 3$, without multiple factors. Let $m \in \mathbb{K}^*$ and let S be a finite set of places of $\mathbb{K}$. Then the equation*

$$f(X, Y) = m$$

has at most finitely many solutions $(X, Y) = (a, b) \in O^2_{\mathbb{K},S}$.

Proof. See [17, chapter I]. □

Roth's theorem was extended by Schmidt in 1970 to system of inequalities in linear forms in the celebrated *Schmidt's subspace theorem*. In this case infinitely many solutions may arise, but all of them are contained in a finite union of proper linear subspaces. Later on Schlickewei obtained a generalization of Schmidt's theorem, analogous to Lang's generalization 1.7 of Roth's theorem. To state the subspace theorem in the generalized form by Schlickewei, let us introduce the following notation: for a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{K}^n$ and a place $\mu \in M_\mathbb{K}$, we set $|\mathbf{x}|_\mu = \max_i |x_i|_\mu$.

Theorem 1.9 (Schmidt, Schlickewei)**.** *Let $\mathbb{K}$ be a number field and let S be a finite set of places, including the archimedean ones. For each $\mu \in S$, let $L_{i\mu}$, $i = 1, \ldots, n$, be n linearly independent linear forms in n variables with $\mathbb{K}$-algebraic coefficients. Then, for every $\epsilon > 0$, the solutions $\mathbf{x} \in O^n_{\mathbb{K},S}$ to the inequality*

$$\prod_{\mu \in S} \prod_{i=1}^{n} \left|L_{i\mu}(\mathbf{x})\right|_\mu \leq H(\mathbf{x})^{-\epsilon}$$

all lie in a certain finite union of proper linear subspaces of $\mathbb{K}^n$.

Proof. See [7] or [8]. □

1.4 Applications

Let now $\mathbb{K}$ be a number field, let S be a finite set of places, including the archimedean ones, and let $O^*_{\mathbb{K},S}$ be the group of S-units of $\mathbb{K}$. Then a classical application of Theorem 1.7 is the following result. *S-unit equation*

$$x + y = 1 \tag{1.11}$$

has only finitely many solutions $x, y \in O^*_{\mathbb{K},S}$. A proof can be found in [9, part D] and uses strongly Theorem 1.7 and the fact that, for any positive rational integer m, the quotient group $O^*_{\mathbb{K},S}/mO^*_{\mathbb{K},S}$ is finite. The finiteness of solutions of the S-unit equation was however originally proved, prior to Roth's theorem, by Siegel in the case S consists of the set of archimedean places of $\mathbb{K}$ and extended by Mahler to arbitrary S. As a generalization of this result, consider a more general S-unit equation

$$x_1 + x_2 + \ldots + x_n = 1 \tag{1.12}$$

to be solved in $\left(O^*_{\mathbb{K},S}\right)^n$. As an application of Theorem 1.9, Evertse, van der Poorten and Schlickewei showed that equation (1.12) has only finitely many non-degenerate (i.e. no subsum on the left hand side vanishes) solutions. A proof of this result can be found in [17, chapter II].

Let us now consider the applications of Theorem 1.9, that led to this thesis.

Definition 1.10. Two algebraic numbers $a, b \in \mathbb{C}$ are multiplicatively dependent if and only if there exists $(h, k) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ such that $a^h b^k = 1$.

As an application of Theorem 1.9, in the particular case $\mathbb{K} = \mathbb{Q}$, Bugeaud, Corvaja and Zannier proved in [3] the following theorem.

Theorem 1.11 (Bugeaud, Corvaja and Zannier)**.** *Let a, b be multiplicatively independent integers ≥ 2 and let $\epsilon > 0$. Then, provided n is sufficiently large, we have*

$$\gcd\left(a^n - 1, b^n - 1\right) < \exp(\epsilon n). \tag{1.13}$$

Corvaja and Zannier then observed in [5], that a combination of the arguments therein contained with the more refined technique of [3], leads to the following sharpening of Theorem 1.11.

Theorem 1.12 (Corvaja and Zannier)**.** *Let $\epsilon > 0$ and let S be a finite set of absolute values of $\mathbb{Q}$, including the archimedean one. Then,*

$$\gcd\left(u - 1, v - 1\right) \ll_{\epsilon,S} \max\{|u|, |v|\}^{\epsilon} \tag{1.14}$$

for every u, v multiplicatively independent S-units of $\mathbb{Z}$.

Proof. See [17, chapter IV]. □

Then a further analysis led to a generalization of these results in terms of heights of algebraic numbers. In [6], Corvaja and Zannier generalized the upper bound for the greatest common divisor to more general pairs of rational functions other than $\{u-1, v-1\}$. As a corollary of the main result of [6], they proved the following proposition (beware that our definition of $\log^-$ differs from that of [6], where $\log^- x = \min\{0, \log x\}$).

Proposition 1.13 (Corvaja and Zannier. Proposition 2 of [6])**.** *Let $\delta > 0$. All but finitely many solutions $(u, v) \in (O^*_{\mathbb{K},S})^2$ to the inequality*

$$\sum_{\mu \in M_0} \log^- \max\{|u-1|_\mu, |v-1|_\mu\} > \delta \max\{h(u), h(v)\}$$

satisfy one of finitely many relations $u^a v^b = 1$, where $a, b \in \mathbb{Z}$ are not both zero.

This diophantine approximation result will be a fundamental tool in proving our results in chapter 3. Our main theorem (Theorem 3.4) in chapter 3 will be a generalization of the following result, proved by Corvaja, Rudnick and Zannier in [4]. Let A be a $d \times d$ non singular integer matrix and let $N \geq 1$ be an integer.

Definition 1.14. The *order*, or *period*, of A modulo N is the smallest positive integer k such that all the entries of $A^k - I$, where I denotes the $d \times d$ identity matrix, are divisible by N. In compact notation

$$A^k \equiv I \pmod{N}.$$

The order of A modulo N will be denoted by $\mathrm{ord}(A, N)$. If A is not invertible modulo N, we set $\mathrm{ord}(A, N) = \infty$.

The main result of [4] is the following theorem.

Theorem 1.15 (Corvaja, Rudnick and Zannier)**.** *Let A be a non singular integer matrix. Then*

$$\lim_{N \to +\infty} \frac{\mathrm{ord}(A, N)}{\log N} = +\infty$$

if and only if none of the following cases holds:

(i) A is diagonalizable and a power of A has all the eigenvalues equal to powers of a single rational integer.

(ii) A is diagonalizable and a power of A has all the eigenvalues equal to powers of a single unit in a real quadratic field.

In chapter 3 we will generalize this theorem and our target will be to formulate a more general result in this context. Instead of searching a minimum k such that all the entries of $A^k - I$ are divisible by N, we will fix an integer r between 0 and d and study the behaviour, as N approaches infinity, of the minimum integer k such that the N-rank of $A^k - I$, which will be defined in chapter 3, becomes smaller than r. These concepts will be defined rigorously in chapter 3, and the N-rank will play the role of the usual rank, when one considers the matrices modulo N. Theorem 1.15 will be recovered in the case $r = 0$.

Chapter 2

Elliptic curves

2.1 Weierstrass model

An *elliptic curve* E is a non singular projective curve of genus 1 with a distinguished point O. Let now $\mathbb{K}$ be a field; if E, as an algebraic curve, is defined over $\mathbb{K}$ and $O \in E(\mathbb{K})$, then the elliptic curve E is said to be *defined over* $\mathbb{K}$. Every such curve can be written as the zero set of a homogeneous polynomial in three variables, i.e. every elliptic curve has a plane model in $\mathbb{P}_2(\mathbb{K})$, defined by an equation of the form

$$Y^2Z + aXYZ + bYZ^2 = X^3 + cX^2Z + dXZ^2 + eZ^3 \tag{2.1}$$

where the coefficients a, b, c, d, e belong to $\mathbb{K}$. Such an equation is called a Weierstrass model of E. Setting $Z = 0$, it is immediate to see that there is only one point O on the line at infinity,

$$O = (0 : 1 : 0)$$

and this is the aforementioned distinguished point. More precisely, given a smooth projective curve E of genus 1 defined over a field $\mathbb{K}$ and a point $O \in E(\mathbb{K})$, there exist two rational functions $x, y \in \mathbb{K}(E)$ such that the rational map

$$\begin{aligned} \phi : E &\longrightarrow \mathbb{P}_2(\mathbb{K}) \\ P &\longmapsto (x(P) : y(P) : 1) \end{aligned}$$

extends to an isomorphism of E into a plane curve given by a Weierstrass equation (2.1).
In affine coordinates x, y, (2.1) becomes

$$y^2 + axy + by = x^3 + cx^2 + dx + e \tag{2.2}$$

and when $\mathrm{char}(\mathbb{K}) \neq 2, 3$ a change of variables can put (2.2) into the simpler form

$$y^2 = x^3 + Ax + B \tag{2.3}$$

where A, B are linked to a, b, c, d, e by the relations

$$\begin{aligned} A &= -27\left((a^2+4c)^2 - 24(2d+ab)\right) \\ B &= -54\left(-(a^2+4c)^3 + 36(a^2+4c)(2d+ab) - 216(b^2+4e)\right) \end{aligned}$$

The quantity

$$\Delta = -16(4A^3 + 27B^2) \tag{2.4}$$

is called the *discriminant* of the cubic curve, and the curve is non singular if and only if $\Delta \neq 0$. Singular cubic curves are much easier to study from an arithmetic viewpoint, since the following proposition holds.

Proposition 2.1. *A singular cubic curve is birational to* $\mathbb{P}_1$.

Proof. See [16, chapter III] □

From now on we will consider only non singular curves.

2.2 Group law

Let E be an elliptic curve defined by a Weierstrass equation (2.1). By Bezout theorem, a line in $\mathbb{P}_2$ intersects E in exactly three points, if we count the points with their intersection multiplicity. With this fact in mind we can define a binary operation on E, which is called *addition*, as follows. Let $P, Q \in E$ and let R be the third point on E which belongs to the line connecting P and Q. Then $P + Q$ is the third point of intersection of the line connecting O and R with E; in fig. 2.1 we can see what happens when we add two real points on E. The curve E equipped with this binary operation becomes an abelian group and the only non trivial part to prove is the associativity of the addition (see [16, chapter III] for a proof based on the Riemann-Roch theorem). Indeed it can be proven that the group law (and its associativity) and the Riemann-Roch theorem for elliptic curves are essentially equivalent (see [12, Section 11.9]). Let us now define the concept of *rational point*.

Definition 2.2. If E is an elliptic curve defined over a field $\mathbb{K}$, then the set

$$E(\mathbb{K}) = \left\{P \in E | P = (x, y) \in \mathbb{K}^2\right\} \cup \{O\},$$

endowed with the restriction of the addition on E, is a subgroup of E, called the group of $\mathbb{K}$-rational points, or simply the group of rational points, when the field is clear from the context.

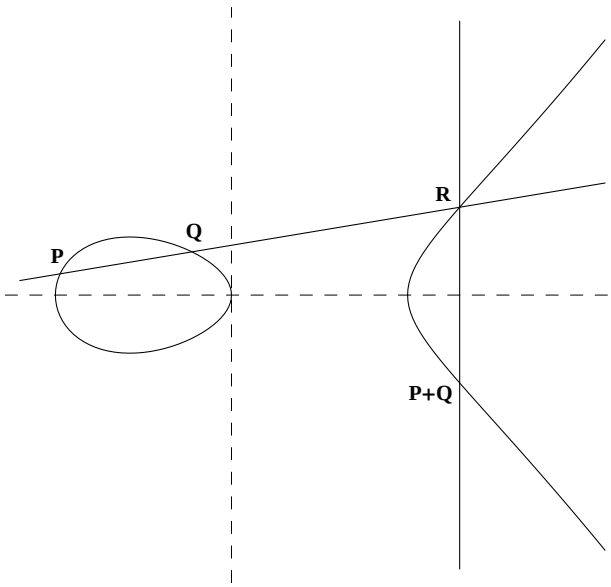

Figure 2.1: *Group law*. The line connecting P and Q intersects E in a third point R. The vertical line through R represents the affine part of the projective line connecting R and the point at infinity on E. This line intersects E in a third point, which is $P+Q$.

2.3 Isogenies

Definition 2.3. Given two elliptic curves E_1, E_2, an *isogeny* between E_1 and E_2 is a morphism

$$\phi : E_1 \longrightarrow E_2$$

such that $\phi(O) = O$. If the isogeny is not trivial, i.e. if $\phi(E_1) \neq \{O\}$ then the two curves are said to be *isogenous*.

Since the points of an elliptic curve form a group under the addition law defined in section 2.2, it would be interesting to characterize the isogenies that are group homomorphisms. The following theorem answers this question.

Theorem 2.4. *Every isogeny is a group homomorphism.*

Proof. See [16, chapter III] □

Since every morphism of algebraic curves is either constant or surjective, then so is every isogeny between elliptic curves. The set $\mathrm{Hom}(E_1, E_2)$ of isogenies between two curves E_1 and E_2 is a group under the addition

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

and if the two curves are equal, let us say to E, then we can also compose isogenies to form a ring $\mathrm{End}(E) = \mathrm{Hom}(E, E)$, the *endomorphism ring* of E. The invertible elements of $\mathrm{End}(E)$ form a group $\mathrm{Aut}(E)$, the *automorphism group* of E.
For every $m \in \mathbb{Z}$ let us now define the isogeny *multiplication by m*, and denote it by $[m]$, as follows

$$\begin{aligned} [m] : E &\longrightarrow E \\ P &\longmapsto \begin{cases} \underbrace{P + P + \ldots + P}_{m-\text{times}}, & \text{if } m > 0 \\ 0, & \text{if } m = 0 \\ [-m](-P), & \text{if } m < 0 \end{cases} \end{aligned}$$

These maps are always non constant if $m \neq 0$ (see [16, chapter III]) and they are the unique evident endomorphisms for an arbitrary elliptic curve; as such they are a fundamental tool in studying elliptic curves. When $m \neq 0$,

$$E[m] = \mathrm{Ker}[m] = \left\{ P \in E\left(\overline{\mathbb{K}}\right) | [m]P = O \right\}$$

is a subgroup of E, called the subgroup of m-torsion points. The following proposition gathers the main properties of the multiplication by m and m-torsion subgroups.

Proposition 2.5. *If E is an elliptic curve defined over $\mathbb{K}$ and m is a non zero integer, then*

(i) $\deg[m] = m^2$, *where* $\deg[m]$ *is the degree of the map* $[m]$.

(ii) If $char(\mathbb{K}) = 0$ *or if m is coprime with* $char(\mathbb{K})$, *then*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$$

(ii) If $char(\mathbb{K})|m$, *then either*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \qquad or \qquad E[m] \cong \{O\}$$

Proof. See [16, chapter III] □

2.4 Tate module

Let $\mathbb{K}$ be a field and let $\overline{\mathbb{K}}$ be an algebraic closure. If E is an elliptic curve defined over $\mathbb{K}$ and $m > 1$ is an integer, coprime with $\mathrm{char}(\mathbb{K})$ if $\mathrm{char}(\mathbb{K}) > 0$, then by Proposition 2.5,

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) .$$

Hence, by choosing a basis for $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, the automorphism group of the $\mathbb{Z}$-module $E[m]$ verifies:

$$\mathrm{Aut}\,(E[m]) \cong \mathrm{GL}_2\,(\mathbb{Z}/m\mathbb{Z})\,.$$

Moreover every element σ of the Galois group $\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$ acts on $E[m]$, since, for every $P \in E[m]$,

$$[m]\,(\sigma(P)) = \sigma\,([m]P) = \sigma(O) = O.$$

Therefore we obtain a representation

$$\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right) \longrightarrow \mathrm{GL}_2\,(\mathbb{Z}/m\mathbb{Z})\,.$$

This representation is not completely satisfactory, since it is usually easier to deal with representations whose matrices have coefficients in a ring of characteristic 0. This observation suggests the following definition.

Definition 2.6. Let E be an elliptic curve and let $l \in \mathbb{Z}$ be a prime. For every integer $n \geq 1$, the multiplication by l is a map from $E[l^{n+1}]$ into $E[l^n]$. With respect to these maps we construct the inverse limit

$$T_l(E) = \varprojlim_n E[l^n]$$

and call it the l-adic Tate module of E.

The group $T_l(E)$ has a natural structure of $\mathbb{Z}_l$-module and, by proposition 2.5,

$$T_l(E) \cong \begin{cases} \mathbb{Z}_l \times \mathbb{Z}_l, & \text{if } l \neq \mathrm{char}(\mathbb{K}) \\ \{O\} \quad or \quad \mathbb{Z}_l, & \text{if } l = \mathrm{char}(\mathbb{K}) > 0 \end{cases} \tag{2.5}$$

Since the following diagram commutes for every $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$

$$\begin{array}{ccc} E[l^{n+1}] & \xrightarrow{[l]} & E[l^n] \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ E[l^{n+1}] & \xrightarrow{[l]} & E[l^n] \end{array}$$

we see that $\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$ acts also on $T_l(E)$.

Definition 2.7. Let E be an elliptic curve and let $l \in \mathbb{Z}$ be a prime. The l-adic representation ρ_l, of $\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$ on E, is the map

$$\rho_l : \mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right) \longrightarrow \mathrm{Aut}\left(T_l(E)\right),$$

giving the action of $\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$ on $T_l(E)$.

If l is coprime with the characteristic of $\mathbb{K}$, then $\mathrm{Aut}\left(T_l(E)\right) \cong \mathrm{GL}_2\left(\mathbb{Z}_l\right)$ and since $\mathbb{Z}_l \subset \mathbb{Q}_l$, we have a representation of $\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$ over a field of characteristic zero:

$$\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{Q}_l\right).$$

The Tate module is a useful construction to study isogenies, in fact if ϕ is an isogeny from E_1 to E_2, then, for every $n \geq 0$, ϕ induces a map between the corresponding l^n-torsion points, i.e. ϕ induces a map

$$\phi : E_1[l^n] \longrightarrow E_2[l^n]$$

and hence ϕ induces a $\mathbb{Z}_l$-linear map between the corresponding Tate modules:

$$\phi : T_l(E_1) \longrightarrow T_l(E_2).$$

If $\phi \in \mathrm{End}(E)$, then we have a ring homomorphism

$$\mathrm{End}(E) \longrightarrow \mathrm{End}\left(T_l(E)\right) \tag{2.6}$$

which is indeed a Galois module homomorphism.

2.5 Elliptic curves over finite fields

Let now $\mathbb{F}_q$ be a finite field, with q elements, of characteristic $p > 0$. Let ϕ_q be the Frobenius endomorphism of $\mathbb{F}_q$, i.e. let ϕ_q be the map

$$\begin{array}{rcl} \phi_q : \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & x^q. \end{array}$$

We can extend ϕ_q to an algebraic closure $\overline{\mathbb{F}}_q$ with the same definition and the points of $\overline{\mathbb{F}}_q$ that belong to $\mathbb{F}_q$ are precisely those that are fixed by ϕ_q. In the same way, given an elliptic curve E defined over $\mathbb{F}_q$, we can define the *Frobenius endomorphism* ϕ_q of E as, in the affine plane,

$$\begin{array}{rcl} \phi_q : E & \longrightarrow & E \\ (x, y) & \longmapsto & (x^q, y^q). \end{array}$$

Then the set of $\mathbb{F}_q$-rational points is precisely the set fixed by the Frobenius endomorphism:

$$E\left(\mathbb{F}_q\right) = \left\{P \in E \mid \phi_q(P) = P\right\}.$$

The same holds in a finite extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$; in this case the set of $\mathbb{F}_{q^n}$-rational points of E, is precisely the set of points of E that are fixed by

$$\phi_q^n = \underbrace{\phi_q \circ \phi_q \circ \ldots \circ \phi_q}_{n\text{-times}}.$$

From now on we will drop the subscript q from ϕ_q, when this will be clear from the context, and we will write simply ϕ. The Frobenius endomorphism is purely inseparable and has degree q. More generally one can prove the following proposition.

Proposition 2.8. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let ϕ be its Frobenius endomorphism. Then, for every $m, n \in \mathbb{Z}$, the map*[1]

$$m + n\phi : E \longrightarrow E$$

is inseparable if and only if $char(\mathbb{F}_q) \mid m$.

Let us now consider a prime $l \neq \text{char}(\mathbb{F}_q)$. Since (2.6) holds, then to every $\psi \in \text{End}(E)$ we can associate an endomorphism of the Tate module of E:

$$\begin{array}{ccc} \text{End}(E) & \longrightarrow & \text{End}\left(T_l(E)\right) \\ \psi & \longmapsto & \psi_l \end{array}$$

and since l is coprime with $\text{char}(\mathbb{F}_q)$, then, recalling (2.5), by choosing a $\mathbb{Z}_l$-basis for $T_l(E)$, we can associate to ψ_l a 2×2 matrix and compute its determinant $\det(\psi_l)$ and trace $\text{Tr}(\psi_l)$, which *a priori* belong to $\mathbb{Z}_l$, but indeed we can say much more about them, as the following proposition shows.

Proposition 2.9. *Let E be an elliptic curve over $\mathbb{F}_q$ and let l be a prime, distinct from the characteristic of $\mathbb{F}_q$. Then for every $\psi \in End(E)$,*

$$\begin{aligned} \det(\psi_l) &= \deg(\psi) \\ Tr(\psi_l) &= 1 + \deg(\psi) - \deg(1 - \psi) \end{aligned}$$

Proof. See [16, chapter V]. □

Thus $\det(\psi_l)$ and $\text{Tr}(\psi_l)$ are rational integers and do not depend on l; we will use this fact extensively in chapter 4. Let us now consider again the q-th Frobenius ϕ of E: by proposition 2.8, the map $1 - \phi^n$ is separable for every $n \geq 1$. Since for a non

[1] $m + n\phi$ is a short notation for $[m] + [n] \circ \phi$ where $+$ is the addition on the elliptic curve.

constant isogeny ψ, $\sharp\phi^{-1}(P) = \deg_s(\psi)$ (separable degree of ψ), we have that if ψ is separable,

$$\sharp\ker(\psi) = \deg(\psi).$$

If we apply this fact to $\psi = 1 - \phi$, then

$$\sharp E\left(\mathbb{F}_{q^n}\right) = \deg(1 - \phi^n) = \det(1 - \phi_l^n), \tag{2.7}$$

where the last equality follows from proposition 2.9. Let us now factor over $\mathbb{C}$ the characteristic polynomial of ϕ_l:

$$\det(T - \phi_l) = T^2 - \mathrm{Tr}(\phi_l)T + \det(\phi_l) = (T - \alpha)(T - \beta)$$

Since for every $r/s \in \mathbb{Q}$,

$$\det\left(\frac{r}{s} - \phi_l\right) = \frac{1}{s^2}\det\left(r - s\phi_l\right) = \frac{1}{s^2}\deg\left(r - s\phi\right) \geq 0,$$

we have $\alpha = \overline{\beta}$. Hence $|\alpha| = |\beta|$ and since $\alpha\beta = \det(\phi_l) = \deg(\phi) = q$, then

$$|\alpha| = |\beta| = \sqrt{q}.$$

Hence (2.7) becomes

$$\sharp E\left(\mathbb{F}_{q^n}\right) = \det(1 - \phi_l^n) = 1 - (\alpha^n + \overline{\alpha}^n) + q^n. \tag{2.8}$$

The following estimate on the number $\sharp E\left(\mathbb{F}_{q^n}\right)$ of $\mathbb{F}_{q^n}$-rational points was conjectured by Artin and proved by Hasse in 1934.

Theorem 2.10 (Hasse)**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then*

$$\left|\sharp E\left(\mathbb{F}_{q^n}\right) - q^n - 1\right| \leq 2\sqrt{q^n}. \tag{2.9}$$

Proof. Follows immediately from equation (2.8). □

Theorem 2.10 can be used to estimate certain character sums as follows. Let

$$y^2 = f(x)$$

be the Weierstrass equation of an elliptic curve over $\mathbb{F}_q$. Let

$$\chi : \mathbb{F}_q^* \longrightarrow \{\pm 1\}$$

be the quadratic Legendre character of $\mathbb{F}_q^*$, extended to the hole $\mathbb{F}_q$, by $\chi(0) = 0$. Then

$$\sharp E\left(\mathbb{F}_q\right) = 1 + \sum_{x \in \mathbb{F}_q}\left(\chi\left(f(x)\right) + 1\right),$$

since we have one point at infinity (that's where the '1' comes from) and each $x \in \mathbb{F}_q$ gives contribution 0, 1 or 2 to the sum, respectively when $f(x)$ is a non square, $f(x)$ is zero or $f(x)$ is a non zero square in $\mathbb{F}_q$. Then

$$\sharp E\left(\mathbb{F}_q\right) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi\left(f(x)\right). \tag{2.10}$$

Comparing this equation with (2.9), we obtain

$$\left| \sum_{x \in \mathbb{F}_q} \chi\left(f(x)\right) \right| \leq 2\sqrt{q}.$$

Conversely, without using Theorem 2.10, equation (2.10), together with the trivial bound

$$\left| \sum_{x \in \mathbb{F}_q} \chi\left(f(x)\right) \right| \leq q,$$

provides an upper bound for the number of rational points, that we will use in Chapter 4:

$$\sharp E\left(\mathbb{F}_q\right) \leq 1 + 2q. \tag{2.11}$$

To conclude this section, let us study the group structure of $E\left(\mathbb{F}_{q^n}\right)$ and prove the following fact.

Proposition 2.11. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then there exist two positive rational integers $m(q^n), l(q^n)$, with $m(q^n) \mid l(q^n)$ such that*

$$E(\mathbb{F}_{q^n}) \cong (\mathbb{Z}/m(q^n)\mathbb{Z}) \times (\mathbb{Z}/l(q^n)\mathbb{Z})$$

Proof. The group $E(\mathbb{F}_{q^n})$ is a finite abelian group, then, by the structure theorem for such groups, there exist positive integers $n_1, n_2, \ldots n_k$, with $n_i \mid n_{i+1}$ for every $i = 1, 2, \ldots, k-1$, such that

$$E(\mathbb{F}_{q^n}) \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots (\mathbb{Z}/n_k\mathbb{Z})$$

In particular every n_i is a multiple of n_1. Observe now that in a group of the form $\mathbb{Z}/nm\mathbb{Z}$, with n, m positive integers, we have exactly n points whose order divides n (i.e. points of n-torsion), hence each $\mathbb{Z}/n_i\mathbb{Z}$ contains exactly n_1 points of n_1-torsion. Therefore, if $E(\mathbb{F}_{q^n})$ has the form (2.5), it possesses n_1^k points of n_1-torsion. But, since proposition 2.5 holds, E has at most n_1^2 points of n_1-torsion. We conclude that $k \leq 2$ and the assertion follows. □

2.6 Supersingular and ordinary elliptic curves

For a given elliptic curve E over $\mathbb{F}_q$, $q = p^k$, by Proposition 2.5 we have two possibilities for the group of p-torsion points, namely

$$E[p] \cong \begin{cases} (\mathbb{Z}/p\mathbb{Z}) \\ \\ \{O\} \end{cases} \quad \text{or}$$

In the first case the elliptic curve is called *ordinary* and in the second case *supersingular*. Beware that the notion of supersingularity is completely different from the notion of singularity, in particular a supersingular elliptic curve is still a non singular algebraic curve. There exist many different characterizations of supersingular elliptic curves and we refer the reader to [11, chapter 13] for a thorough treatment. We mention here only the following characterization, in terms of the Frobenius endomorphism, that we will use in chapter 4.

Proposition 2.12. *If E is an elliptic curve defined over $\mathbb{F}_q$, then E is supersingular if and only if there exist two positive integers a, b such that $\phi^a = [p^b]$, where $p = char(\mathbb{F}_q)$.*

Proof. See [11, chapter 13]. □

Chapter 3

The r-order of a matrix

3.1 Definitions

Recall that, as explained in chapter 1, Corvaja, Rudnick and Zannier proved in [4] that for a non singular integer matrix A, the growth of the order of A modulo an integer N goes to infinity faster then $\log N$ if and only if none of the following cases holds:

(i) A is diagonalizable and a power of A has all the eigenvalues equal to powers of a single rational integer

(ii) A is diagonalizable and a power of A has all the eigenvalues equal to powers of a single unit in a real quadratic field

Let now d be a positive integer and A a non singular $d \times d$ integer matrix. Given an integer $N \geq 1$, we define the N-rank of A as follows.

Definition 3.1. The N-rank of A is the greatest integer $r \geq 0$ such that there exists an $r \times r$ minor of A whose determinant is not divisible by N. We will write $r = N\text{-rank}(A)$.

Given r as in definition 3.1 we can define the *r-order* of the matrix A as follows.

Definition 3.2. A positive integer k is called the r-order of A modulo N, if it is the smallest integer such that $N\text{-rank}(A^k - I) \leq r$, where I denotes the identity matrix. We will write $k = \text{ord}(A, N, r)$. If such an integer does not exist, we will set $\text{ord}(A, N, r) = \infty$.

3.2 Properties of the r-order and the N-rank

Before stating the main results of this thesis, we briefly analyze the main properties of N-rank and r-order. An integer matrix A has N-rank zero if and only if all the minors of order 1 are divisible by N, i.e. if and only if $A \equiv 0 \pmod{N}$. Hence $\mathrm{ord}(A, N, 0)$ is just the usual order $\mathrm{ord}(A, N)$ of a matrix and has been studied in [4] as recalled above. Recall now that from an integer $d \times d$ matrix $A = (a_{ij})$ and a given positive integer $r \leq d$, one can construct a new matrix, the so called r-th exterior power of A as follows. Let S_r^d be the set of r-tuples

$$J = (j_1, j_2, \ldots, j_r), \quad \text{where } 1 \leq j_1 < j_2 < \ldots < j_r \leq d$$

and let $J, K \in S_r^d$. Then we define

$$A_{J,K}^{(r)} := \det \begin{pmatrix} a_{j_1k_1} & a_{j_1k_2} & \cdots & a_{j_1k_r} \\ a_{j_2k_1} & a_{j_2k_2} & \cdots & a_{j_2k_r} \\ \vdots & \vdots & & \vdots \\ a_{j_rk_1} & a_{j_rk_2} & \cdots & a_{j_rk_r} \end{pmatrix}. \tag{3.1}$$

Hence, by varying J, K in S_r^d we obtain, after choosing an enumeration for the elements of S_r^d, a new matrix $A^{(r)}$, the r-th exterior power of A, whose JK-component is defined by (3.1). Choose now a $\mathbb{Z}$-basis $\{e_1, e_2, \ldots, e_d\}$ for $\mathbb{Z}^d$; then the elements

$$e_J = e_{j_1} \wedge e_{j_2} \wedge \ldots \wedge e_{j_r}, \quad \text{where } J = (j_1, j_2, \ldots, j_r) \in S_r^d,$$

form a basis of the exterior power $\bigwedge^r \mathbb{Z}^d$ and the matrix $A^{(r)}$ represents the endomorphism

$$\bigwedge^r A : \bigwedge^r \mathbb{Z}^d \longrightarrow \bigwedge^r \mathbb{Z}^d.$$

Now $N\text{-rank}(A) \leq r$ if and only if every determinant of a minor of order $r+1$ is divisible by N and this in turn is equivalent to the fact that the matrix $A^{(r+1)}$, representing $\bigwedge^{r+1} A$, has all the entries divisible by N, i.e. $N | A^{(r+1)}$. Moreover, if one defines, for $0 \leq r \leq d$, the determinant ideal $I_r(A)$ to be the ideal in $\mathbb{Z}$ generated by the entries of $A^{(r)}$, i.e. by the determinants of the minors of A of order r, then, after putting $I_0(A) := \mathbb{Z}$,

$$I_0(A) \supset I_1(A) \supset \cdots \supset I_d(A).$$

It follows that, for every r between 0 and $d-1$,

$$\mathrm{ord}(A, N, r) \geq \mathrm{ord}(A, N, r+1). \tag{3.2}$$

Let now $P, Q \in \mathrm{GL}_d(\mathbb{Z})$. In this case $I_r(P) = I_r(Q) = (1)$ for every r, hence, since for two $d \times d$ integer matrices A, B,

$$(AB)^{(r)} = A^{(r)} B^{(r)},$$

then

$$I_r(A) = I_r(PAQ)$$

and we deduce that the N-rank is invariant under conjugation in GL_d.

3.3 Statements of the results

In this thesis we study the minimal growth of $\mathrm{ord}(A, N, r)$, for fixed values of r and given A, as $N \to \infty$. If A has finite r-order (globally), i.e. $A^k - I$ has rank at most r for a certain $k \geq 1$, then clearly $\mathrm{ord}(A, N, r) \leq k$ is bounded. If this is not the case, then $\mathrm{ord}(A, N, r) \to \infty$ as $N \to \infty$.
The case $r = d$ is trivial, being $\mathrm{ord}(A, N, d) = 1$ for each integer $N \geq 1$. When $r = d - 1$ the growth is not faster then logarithmic on a subsequence, as we shall now prove. Let us first consider the case where no eigenvalue is a root of unity. Let $\lambda_1, \ldots, \lambda_t, \lambda_{t+1}, \ldots \lambda_d$ be the complex eigenvalues of A, each repeated as many times as its algebraic multiplicity and ordered in a way that $|\lambda_i| > 1$ if and only if $i \leq t$. Let $N_n = |\det(A^n - I)| = (\lambda_1^n - 1) \cdots (\lambda_d^n - 1)$ and $\eta = \sum_{i=1}^t \log |\lambda_i|$. Observe that

$$\log N_n = \sum_{i=1}^{t} \log \left|\lambda_i^n - 1\right| + O(1) = n\eta + O(1) \tag{3.3}$$

and recall that $\mathrm{ord}(A, N_n, d-1)$ is the smallest integer k such that $N_n\text{-rank}(A^k - I) \leq d - 1$, i.e. k is the smallest integer such that N_n divides $\det(A^k - I)$. Since N_n divides $\det(A^n - I)$, then we have that $k \leq n$ and, using (3.3), we obtain

$$\mathrm{ord}(A, N_n, d-1) \leq n = \eta^{-1} \log N_n + O(1)$$

and so

$$\liminf_{N \to \infty} \frac{\mathrm{ord}(A, N, d-1)}{\log N} \leq \eta^{-1} < \infty$$

as wanted.
If an eigenvalue, say λ_1, is a root of unity, with $\lambda_1^m = 1$, then $\det(A^m - I) = 0$, and therefore we have $\mathrm{ord}(A, N, d-1) \leq m$ for every positive integer N.

From now on we will then consider $0 \leq r \leq d - 2$. Let $\mathbb{K} \subset \overline{\mathbb{Q}}$ be the splitting field of the characteristic polynomial of A. Then there exists an invertible matrix P over $\mathbb{K}$ such that

$$B = P^{-1}AP \tag{3.4}$$

is the Jordan canonical form of A. Let now Λ be the set of eigenvalues of A, let $\Lambda^* \subset \Lambda$ be the set of eigenvalues that are roots of unity and let $\Lambda' := \Lambda \setminus \Lambda^*$. Let $\sim$ be the equivalence relation of being multiplicatively dependent, defined on the

set Λ' of eigenvalues of A which are not roots of unity and let $\Gamma := \Lambda'/\sim$. Note that $\sim$ would not be an equivalence relation if defined on the whole Λ, since every eigenvalue is multiplicatively dependent with an eigenvalue in Λ^* and transitivity would fail. For each equivalence class $\gamma \in \Gamma$ we set h_γ to be the sum of the algebraic multiplicities of the eigenvalues in γ and $\overline{h}_\gamma$ to be the number of 1's appearing in the Jordan blocks of B relative to the eigenvalues in γ. Finally let l be the sum of the algebraic multiplicities of the eigenvalues in Λ^* and $\bar{l}$ be the number of 1's appearing in the Jordan blocks of B relative to the eigenvalues in Λ^*.

Definition 3.3. Given an integer r, with $0 \leq r \leq d-2$, a $d \times d$ integer matrix A will be called r-regular if

$$\lim_{N\to\infty} \frac{\operatorname{ord}(A, N, r)}{\log N} = +\infty \tag{3.5}$$

and r-exceptional otherwise.

The main result of this thesis is the following theorem.

Theorem 3.4. *Let A be a non singular integer $d \times d$ matrix and $r \leq d-2$ a non negative integer. Then A is r-exceptional if and only if there exists $\gamma \in \Gamma$ such that*

$$l - \bar{l} + h_\gamma - \overline{h}_\gamma \geq d - r. \tag{3.6}$$

Note that $l - \bar{l}$ represents the sum of the dimensions of the eigenspaces relative to eigenvalues that are roots of unity, and similarly that $h_\gamma - \overline{h}_\gamma$ represents the sum of the dimensions of the eigenspaces relative to eigenvalues that belong to γ.

Example 3.5. Consider for example the matrix

$$A = \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

This matrix, already in Jordan canonical form, has two multiplicatively independent eigenvalues, both not roots of unity, therefore $l = \bar{l} = 0$ and $h_2 = 1$, $\overline{h}_2 = 0$, $h_3 = 3$, $\overline{h}_3 = 1$. Then, by applying Theorem 3.4, the matrix A is 2-exceptional, 1-regular and then 0-regular, by equation (3.2).

Example 3.6. Consider now an invertible integer matrix whose Jordan form is

$$A = \begin{pmatrix} \zeta_1 & 0 & 0 & 0 & 0 \\ 0 & \zeta_2 & 0 & 0 & 0 \\ 0 & 0 & a & 1 & 0 \\ 0 & 0 & 0 & a & 0 \\ 0 & 0 & 0 & 0 & b \end{pmatrix},$$

where ζ_1, ζ_2 are roots of unity and a, b are two multiplicatively dependent non roots of unity. In this case $l = 2$, $\bar{l} = 0$ and, in the notation of example 3.5, $h_{\bar{a}} = 3$, $\overline{h}_{\bar{a}} = 1$. Then, $l - \bar{l} + h_{\bar{a}} - \overline{h}_{\bar{a}} = 4$, hence by applying Theorem 3.4, the matrix A is 0-regular and 1-exceptional (and then 2- and 3-exceptional, since (3.2) holds).

The main tool to prove the necessity of condition (3.6) for A being $r-$exceptional will be proposition 1.13 by Corvaja and Zannier which is an application of Schmidt's subspace theorem. On the other hand, to prove the sufficiency of (3.6), a generalized version of Roth's theorem will suffice.
As an immediate corollary of Theorem 3.4 we can deduce a sufficient condition on the structure of the Zariski closure $G_A := \overline{< A >}$ in GL_d of the cyclic group generated by a single invertible integer matrix A, for A being r-regular. Let G_A^0 be the connected component of G_A containing the identity; then, by the general theory of commutative algebraic groups, $G_A^0 \cong \mathbb{G}_m^e \times \mathbb{G}_a^f$, where $\mathbb{G}_m$ and $\mathbb{G}_a$ denote respectively the multiplicative and the additive groups and $f = 0$ or 1 depending on A being diagonalizable or not (see [2, chapter I] or [10, chapter 15]).

Corollary 3.7. *Let A be an invertible integer matrix, $r \leq d - 2$ a non negative integer and $G_A^0 \cong \mathbb{G}_m^e \times \mathbb{G}_a^f$ the connected component containing the identity of the Zariski closure of the group generated by A. If $e + f > r + 1$, then A is r-regular.*

The converse of the corollary is not true. Consider for example a 3×3 diagonalizable matrix A with three distinct eigenvalues λ, μ, ν non multiplicatively dependent in pairs, but such that there exist three integers a, b, c with $\lambda^a \mu^b \nu^c = 1$, for instance $\lambda = 3, \mu = 5, \nu = 15$. Then A is 1-regular, but $e + f = 2$.

For certain applications it is more convenient to consider, more generally then an integer matrix, an endomorphism ϕ of a finitely generated free module over a ring of characteristic zero, without choosing a base. If all the coefficients of the characteristic polynomial of ϕ are rational integers, then such are the coefficients of the characteristic polynomial of $\phi^n - I$, for every positive integer n, where I is the identity endomorphism. In the following the coefficients of the characteristic polynomial of an endomorphism ϕ, will be called the *invariants* of ϕ. Let us, for every $k = 1, \ldots, d$, denote by $\alpha_{n,k}$ the invariant of $\phi^n - I$ which is homogeneous of degree k in the eigenvalues of $\phi^n - I$. Recall that

$$\alpha_{n,k} = (-1)^k \mathrm{Tr}\left(\bigwedge^k (\phi^n - I) \right).$$

We can then consider, for fixed $N \in \mathbb{N}$, the smallest positive integer $k(\phi, N)$ such that N divides $\alpha_{n,k}^{d!k^{-1}}$ for all $k = 1, \ldots, d$. A slight modification of the arguments used in proving Theorem 3.4 leads to the following result.

Theorem 3.8. *Let ϕ be an endomorphism of a finitely generated free module over a ring of characteristic zero, such that the invariants of ϕ are rational integers. Then $k(\phi, N)$, defined as above, satisfies*

$$\lim_{N\to\infty} \frac{k(\phi, N)}{\log N} = +\infty \tag{3.7}$$

if and only if ϕ has at least two multiplicatively independent eigenvalues.

Theorems 3.4 and 3.8 will be applied in chapter 4 to the study of the structure of the group of rational points of elliptic curves over extensions of finite fields. The results therein contained will also provide a criterion for isogeny between two elliptic curves.

3.4 Proofs

To prove Theorem 3.4, we need a few lemmas.

Lemma 3.9. *Let A and r be as in Theorem 3.4, A not of finite global r-order, n a positive integer and let $x_{n,r,i}$, $i = 1, \ldots, \binom{d}{r}^2$ be the determinants of the minors of $A^n - I$ of order r. Then the following statement is equivalent to (3.5),*

$$\forall \epsilon > 0, \quad \gcd_i(x_{n,r+1,i}) < \exp(\epsilon n) \ \textit{for } n \textit{ sufficiently large with respect to } \epsilon. \tag{3.8}$$

Proof. Let $k := \mathrm{ord}(A, N, r)$. Then N divides $x_{k,r+1,i}$ for every i. In particular

$$N \leq \gcd_i(x_{k,r+1,i}), \quad \forall N \in \mathbb{N} \tag{3.9}$$

If condition (3.8) holds, then

$$\gcd_i(x_{k,r+1,i}) < \exp(\epsilon k), \quad \text{for } N \text{ (and thus } k\text{) sufficiently large.}$$

Combining this with (3.9) we obtain

$$\frac{\mathrm{ord}(A, N, r)}{\log N} > \epsilon^{-1}, \quad \text{for } N \text{ sufficiently large}$$

and this implies condition (3.5).
On the other hand if there exist a positive real number ρ and an infinite subset $\mathcal{N}$ of $\mathbb{N}$ such that

$$\gcd_i(x_{n,r+1,i}) \geq \exp(\rho n), \quad \forall n \in \mathcal{N}$$

then, taking $N_n := \gcd_i(x_{n,r+1,i})$, we get

$$\operatorname{ord}(A, N_n, r) \le n \le \frac{1}{\rho} \log \gcd_i(x_{n,r+1,i}) = \frac{1}{\rho} \log N_n$$

and so

$$\frac{\operatorname{ord}(A, N_n, r)}{\log N_n} \le \frac{1}{\rho}, \quad \forall n \in \mathcal{N}.$$

Therefore

$$\lim_{N \to \infty} \frac{\operatorname{ord}(A, N, r)}{\log N} \neq +\infty.$$

□

We recall now briefly, for the reader's convenience, some notation, already defined in chapter 1, related with $\mathbb{K}$, the splitting field of the characteristic polynomial of A. Let M and M_0 be respectively the set of places and finite places of the field $\mathbb{K}$ and normalize the associated absolute values in such a way that the product formula $\prod_{\mu \in M} |x|_\mu = 1$ holds for each $x \in \mathbb{K}^*$. We will also need the absolute logarithmic Weil height $h(x) = \log H(x)$ of a point $x \in \mathbb{K}$, where $H(x) := \prod_{\mu \in M} \max\{1, |x|_\mu\}$. If $\{x_1, \ldots, x_k\} \subset O_{\mathbb{K}}$ is a finite set of algebraic integers of $\mathbb{K}$, we define

$$\log \gcd_i(x_i) := \sum_{\mu \in M_0} \log^- \max_i\{|x_i|_\mu\}$$

to extend the concept of gcd from the rational integers to the ring $O_{\mathbb{K}}$ of algebraic integers of $\mathbb{K}$, where $\log^-(x) := -\min\{0, \log(x)\}$ for every $x > 0$. Finally let S be a finite subset of M, including $M \setminus M_0$, and let

$$O^*_{\mathbb{K},S} = \{x \in \mathbb{K} \text{ such that } |x|_\mu = 1, \forall \mu \notin S\}$$

be the group of S-units of $\mathbb{K}$.

Noting that (3.4) implies $A^n - I = P(B^n - I)P^{-1}$ and letting $y_{n,r,i} \in O_{\mathbb{K}}$, $i = 1, \ldots, \binom{d}{r}^2$ be the determinants of the minors of $B^n - I$ of order r, we observe that condition (3.8) (and thus condition (3.5)) holds if and only if a similar condition holds for the matrix B, i.e. (3.8) is equivalent to

$$\forall \epsilon > 0, \quad \log \gcd_i(y_{n,r+1,i}) < \epsilon n \quad \text{for } n \text{ sufficiently large.} \tag{3.10}$$

To prove the equivalence of (3.8) and (3.10) observe that the entries of P are fixed, independently of the exponent n, and hence have bounded denominators as n varies. So for each $i = 1, \ldots, \binom{d}{r}^2$, $y_{n,r,i}$ is a linear combination of the $x_{n,r,j}$, $j = 1, \ldots, \binom{d}{r}^2$ with coefficients having bounded denominators and so $|y_{n,r,i}|_\mu \le c_\mu \max_j |x_{n,r,j}|_\mu$,

where $c_\mu = 1$ for all but finitely many $\mu \in M$. This implies the equivalence of (3.8) and (3.10).
To prove Theorem 3.4, we begin by considering the special case of two multiplicatively dependent eigenvalues. In this case we can prove the following lemma, whose proof is elementary, in the sense that, it does not use any tool of diophantine approximation.

Lemma 3.10. *Let $\lambda, \eta \in \mathbb{K}^\times$ be multiplicatively dependent algebraic integers, λ being not a root of unity, and $B(\eta)$ be a Jordan block of order $k+1$ with exactly k "1" off-diagonal:*

$$B(\eta) := \begin{pmatrix} \eta & 1 & 0 & \cdots & 0 \\ 0 & \eta & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \eta & 1 \\ 0 & \cdots & \cdots & 0 & \eta \end{pmatrix}$$

Let $C_{n,k}(\eta)$ be the $k \times k$ minor of $B(\eta)^n - I$ made up with the first k rows and columns $2, 3, \ldots, k$. Then

$$\log \gcd(\lambda^n - 1, \det C_{n,k}(\eta)) = O(\log n).$$

Proof. Case 1) Consider first the case where η is not a root of unity. Let a, b be non zero integers such that $\lambda^a = \eta^b$. If $ab < 0$, then λ is a unit and, since $\lambda^n - 1 = -\lambda^n(\lambda^{-n} - 1)$, the ideals generated by $\lambda^n - 1$ and $\lambda^{-n} - 1$ coincide, hence

$$\log \gcd(\lambda^n - 1, \det C_{n,k}(\eta)) = \log \gcd(\lambda^{-n} - 1, \det C_{n,k}(\eta))$$

We can therefore suppose a and b positive, by replacing λ with λ^{-1} if necessary. There exists then an algebraic integer $\xi \in \mathbb{K}\left[\sqrt[b]{\lambda}\right]$ such that $\xi^b = \lambda$ and $\xi^a = \eta$. If we now set $t = \xi^n$ we get

$$\lambda^n - 1 = \xi^{bn} - 1 = t^b - 1$$

and, since $\eta^n = t^a$,

$$\det C_{n,k}(\eta) = \det \begin{pmatrix} n\eta^{n-1} & \binom{n}{2}\eta^{n-2} & \cdots & \cdots & \binom{n}{k}\eta^{n-k} \\ \eta^n - 1 & n\eta^{n-1} & \cdots & \cdots & \binom{n}{k-1}\eta^{n-k+1} \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \eta^n - 1 & n\eta^{n-1} & \binom{n}{2}\eta^{n-2} \\ 0 & \cdots & \cdots & \eta^n - 1 & n\eta^{n-1} \end{pmatrix}$$

$$= \eta^{-k} \det \begin{pmatrix} nt^a & \binom{n}{2}t^a & \cdots & \cdots & \binom{n}{k}t^a \\ t^a - 1 & nt^a & \cdots & \cdots & \binom{n}{k-1}t^a \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & t^a - 1 & nt^a & \binom{n}{2}t^a \\ 0 & \cdots & \cdots & t^a - 1 & nt^a \end{pmatrix},$$

where the last equality follows easily, by induction on k.
It is now convenient to define two polynomials $f, g \in \mathbb{Q}[x,t]$, with x and t algebraically independent over $\mathbb{Q}$, as follows:

$$f(x,t) \coloneqq t^b - 1$$

$$g(x,t) \coloneqq \det \begin{pmatrix} xt^a & \binom{x}{2}t^a & \cdots & \cdots & \binom{x}{k}t^a \\ t^a - 1 & xt^a & \cdots & \cdots & \binom{x}{k-1}t^a \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & t^a - 1 & xt^a & \binom{x}{2}t^a \\ 0 & \cdots & \cdots & t^a - 1 & xt^a \end{pmatrix}$$

where f indeed does not depend on the variable x. Writing $\mathbb{Q}[x,t] = \mathbb{Q}[x][t]$ we regard f and g as polynomials in t with coefficients in $\mathbb{Q}[x]$ and show that they do not have a common factor of positive degree. We show that $g(x,t)$ does not have a non zero complex root in t: let z be a non zero complex number and suppose that $z^a \neq 1$; to show that $g(x,z) \in \mathbb{C}[x]$ is not the zero polynomial in x we show that its term of degree one is not zero. This term is the partial derivative of $g(x,z)$ with respect to x, evaluated it in $x = 0$ and to compute it, recall that the derivative of the

determinant of a matrix, whose columns are $c_1, c_2, \ldots, c_k$, is given by

$$\frac{\partial}{\partial x}\det(c_1, c_2, \ldots, c_k) = \det\left(\frac{\partial c_1}{\partial x}, c_2, \ldots, c_k\right) + \det\left(c_1, \frac{\partial c_2}{\partial x}, c_3, \ldots, c_k\right) + \ldots + \det\left(c_1, c_2, \ldots, \frac{\partial c_k}{\partial x}\right).$$

Hence,

$$\begin{aligned}\left.\frac{\partial}{\partial x}g(x,z)\right|_{x=0} &= \det\begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & \left.\frac{\partial}{\partial x}\left(\binom{x}{k}z^a\right)\right|_{x=0} \\ z^a-1 & 0 & \cdots & \cdots & 0 & \left.\frac{\partial}{\partial x}\left(\binom{x}{k-1}z^a\right)\right|_{x=0} \\ 0 & z^a-1 & 0 & \cdots & 0 & \left.\frac{\partial}{\partial x}\left(\binom{x}{k-2}z^a\right)\right|_{x=0} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & z^a-1 & 0 & \left.\frac{\partial}{\partial x}\left(\binom{x}{2}z^a\right)\right|_{x=0} \\ 0 & \cdots & \cdots & \cdots & z^a-1 & z^a \end{pmatrix} \\ &= (z^a-1)^{k-1}\left.\frac{\partial}{\partial x}\left(\binom{x}{k}z^a\right)\right|_{x=0} \neq 0 \end{aligned} \tag{3.11}$$

for every $z \in \mathbb{C}^\times$ such that $z^a \neq 1$, since $\binom{x}{k} = x(x-1)\ldots(x-k+1)k!^{-1}$ has a simple root at $x = 0$. If $z^a = 1$ then $g(x,z) = x^k$, which again is not the zero polynomial in $\mathbb{Q}[x]$.

On the other hand $t = 0$ cannot be a root of $f(x,t)$, so f and g do not have a common root in t. Then their resultant $Res(f,g)$ in the variable t is a non zero element $r(x) \in \mathbb{Q}[x]$ and there exist two polynomials $\phi, \psi \in \mathbb{Q}[x][t]$ such that

$$\phi(x,t)f(x,t) + \psi(x,t)g(x,t) = r(x).$$

Therefore for every $\mu \in M_0$

$$\begin{aligned} & \max\{|\lambda^n - 1|_\mu, \left|\det C_{n,k}(\eta)\right|_\mu\} = \max\{|f(n,\xi^n)|_\mu, \left|\eta^{-k}g(n,\xi^n)\right|_\mu\} \\ \geq\ & \max\{|f(n,\xi^n)|_\mu, |g(n,\xi^n)|_\mu\} \\ \geq\ & \max\{|f(n,\xi^n)|_\mu, |\phi(n,\xi^n)f(n,\xi^n) + \psi(n,\xi^n)g(n,\xi^n)|_\mu\} \\ =\ & \max\{|f(n,\xi^n)|_\mu, |r(n)|_\mu\} \geq |r(n)|_\mu \end{aligned}$$

Then

$$\begin{aligned}\log\gcd(\lambda^n - 1, \det C_{n,k}(\eta)) &= \sum_{\mu\in M_0}\log^-\max\{|\lambda^n-1|_\mu, \left|\det C_{n,k}(\eta)\right|_\mu\} \\ &\leq \sum_{\mu\in M_0}\log^-|r(n)|_\mu \leq h(r(n)) = O(\log n).\end{aligned}$$

Case 2) If η is an m-th primitive root of unity, then

$$\det C_{n,k}(\eta) = \eta^{-k} \det \begin{pmatrix} n\eta^n & \binom{n}{2}\eta^n & \cdots & \cdots & \binom{n}{k}\eta^n \\ \eta^n - 1 & n\eta^n & \cdots & \cdots & \binom{n}{k-1}\eta^n \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \eta^n - 1 & n\eta^n & \binom{n}{2}\eta^n \\ 0 & \cdots & \cdots & \eta^n - 1 & n\eta^n \end{pmatrix}$$

and this is non zero for every $n \in \mathbb{N}$ sufficiently large. In fact, if $n \equiv 0 \pmod{m}$, then $\det C_{n,k}(\eta) = n^k \eta^{-k} \neq 0$ for every $n \in \mathbb{N}$; otherwise, if $n \not\equiv 0 \pmod{m}$, we can repeat part of the above argument with minor modifications and define a polynomial $g \in \mathbb{Q}[x,t]$, with x and t algebraically independent over $\mathbb{Q}$, as follows:

$$g(x,t) = \det \begin{pmatrix} xt & \binom{x}{2}t & \cdots & \cdots & \binom{x}{k}t \\ t-1 & xt & \cdots & \cdots & \binom{x}{k-1}t \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & t-1 & xt & \binom{x}{2}t \\ 0 & \cdots & \cdots & t-1 & xt \end{pmatrix}$$

so that

$$\det C_{n,k}(\eta) = \eta^{-k} g(n, \eta^n) \tag{3.12}$$

Let n_0 be an integer such that $1 \leq n_0 \leq m$, then $g(x,\eta^n) = g(x,\eta^{n_0})$ for every $n \equiv n_0 \pmod{m}$. Hence, as n varies, we obtain at most m different polynomials $g(x,\eta), g(x,\eta^2) \ldots, g(x,\eta^m) \in \mathbb{C}[x]$ and by (3.11), if $n_0 \not\equiv 0 \pmod{m}$, then

$$\frac{\partial}{\partial x} g(x,\eta^{n_0})\Big|_{x=0} = (\eta^{n_0} - 1)^{k-1} \frac{\partial}{\partial x} \left(\binom{x}{k} \eta^{n_0} \right)\Big|_{x=0} \neq 0$$

and so $g(x,\eta^{n_0})$ is not the zero polynomial in $\mathbb{C}[x]$. Then $g(n,\eta^n) \neq 0$ for every n sufficiently large and then (3.12) implies $\det C_{n,k}(\eta) \neq 0$ for every n sufficiently large. Observe now that, for every $\mu \in M_0$,

$$\max\{|\lambda^n - 1|_\mu, \left|\det C_{n,k}(\eta)\right|_\mu\} \geq \left|\det C_{n,k}(\eta)\right|_\mu = \left|\eta^{-k} g(n,\eta^n)\right|_\mu = |g(n,\eta^n)|_\mu$$

But

$$g(n,\eta^n) = \sum_{i=0}^{k} p_i(n) \eta^{in}$$

where the p_i are polynomials over $\mathbb{Z}$. Then

$$\begin{aligned}
\log \gcd(\lambda^n - 1, \det C_{n,k}(\eta)) &\leq \sum_{\mu \in M_0} \log^- |g(n, \eta^n)|_\mu = \log \prod_{\mu \in M_0} |g(n, \eta^n)|_\mu^{-1} \\
&= \log \prod_{\mu \in M \setminus M_0} |g(n, \eta^n)|_\mu = \log \prod_{\mu \in M \setminus M_0} \left| \sum_{i=0}^{k} p_i(n) \eta^{in} \right|_\mu \\
&\leq \log \prod_{\mu \in M \setminus M_0} \sum_{i=0}^{k} \left| p_i(n) \eta^{in} \right|_\mu = \log \prod_{\mu \in M \setminus M_0} \sum_{i=0}^{k} |p_i(n)|_\mu \\
&\leq \log |p(n)|
\end{aligned}$$

for a suitable polynomial p over $\mathbb{Z}$ and every n sufficiently large. Then

$$\log \gcd(\lambda^n - 1, \det C_{n,k}(\eta)) = O(\log n)$$

and this completes the proof of the lemma. □

We are now in a position to prove the main theorem.

Proof of Theorem 3.4. Case 1) Suppose that $l - \bar{l} + h_\gamma - \overline{h}_\gamma < d - r$, i.e. that

$$d - l - h_\gamma + \bar{l} + \overline{h}_\gamma \geq r + 1, \tag{3.13}$$

for every $\gamma \in \Gamma$. Observe that for a chosen $\gamma \in \Gamma$, say γ_1, we have that $d - l - h_{\gamma_1}$ is the order of the principal minor of $B^n - I$ made of all of the blocks relative to eigenvalues not in $\gamma_1 \cup \Lambda^*$. Moreover $\bar{l} + \overline{h}_{\gamma_1}$ is the sum of the orders of the minors of $B^n - I$ of type $C_{n,k_i}(\lambda_i)$, in the notation of Lemma 3.10, where $\lambda_i \in \gamma_1 \cup \Lambda^*$. Hence the inequality (3.13) amounts to say that there exists a minor, say $y_{n,r+1,1}$, of $B^n - I$ of order $r+1$, which is diagonal in blocks and whose blocks are of type $C_{n,k_i}(\lambda_i)$ where $\lambda_i \in \gamma_1 \cup \Lambda^*$ or principal minors of $B^n - I$ relative to eigenvalues not in $\gamma_1 \cup \Lambda^*$. The minor $y_{n,r+1,1}$ will thus have the form

$$y_{n,r+1,1} = \prod_{i \in \mathcal{I}} \det C_{n,k_i}(\lambda_i) \cdot \prod_{j \in \mathcal{K}} (\eta_j^n - 1), \tag{3.14}$$

where $\mathcal{I}$ is a finite set of indexes, $\lambda_i \in \gamma_1 \cup \Lambda^*$, $\forall i \in \mathcal{I}$ and $\mathcal{K}$ is a finite set of indexes of cardinality $r + 1 - \sum_{i \in \mathcal{I}} k_i$ such that $\eta_j \in \Lambda' \setminus \gamma_1$ for each $j \in \mathcal{K}$.
Let now Ω_0 be the product of the elements of a maximal subset of cardinality at most $r+1$ of diagonal elements $\lambda^n - 1$ of $B^n - I$, where $\lambda \in \gamma_1$, i.e.

$$\Omega_0 = \prod_{j \in \mathcal{L}} (\lambda_j^n - 1)$$

where $\mathcal{L}$ is a finite set of indexes of cardinality at most $r+1$, $\lambda_j \in \gamma_1$ for every $j \in \mathcal{L}$, the λ_j not necessarily distinct. Let $\Omega_1, \dots, \Omega_t$ be the determinants of all the minors of order $\max\{0, r+1-h_{\gamma_1}\}$ chosen from the blocks of the matrix $B^n - I$ not relative to eigenvalues in γ_1 and which do not contain elements $\lambda^n - 1$ with $\lambda \in \Lambda^*$; these minors exist, if $h_{\gamma_1} < r+1$, since $d - l - h_{\gamma_1} + \bar{l} \geq r+1-\bar{h}_{\gamma_1} \geq r+1-h_{\gamma_1}$. Otherwise, if $h_{\gamma_1} \geq r+1$, set $t = 1$ and $\Omega_1 = 1$. As last, in equation (3.14), set $\Omega_{t+1} \coloneqq \prod_{i\in\mathcal{I}} \det C_{n,k_i}(\lambda_i)$ and $\Omega_{t+2} \coloneqq \prod_{j\in\mathcal{K}}(\eta_j^n - 1)$. Then

$$\begin{aligned}\log \gcd_i(y_{n,r+1,i}) &\leq \log \gcd(\Omega_0\Omega_1, \Omega_0\Omega_2, \dots, \Omega_0\Omega_t, \Omega_{t+1}\Omega_{t+2}) \\ &\leq \log \gcd(\Omega_1, \Omega_2, \dots, \Omega_t) + \log \gcd(\Omega_0, \Omega_{t+1}\Omega_{t+2}) \\ &\leq \log \gcd(\Omega_1, \Omega_2, \dots, \Omega_t) + \log \gcd(\Omega_0, \Omega_{t+1}) + \log \gcd(\Omega_0, \Omega_{t+2})\end{aligned}$$

Observe now that

$$\log \gcd(\Omega_0, \Omega_{t+1}) \leq \sum_{j\in\mathcal{L}} \sum_{i\in\mathcal{I}} \sum_{\mu\in M_0} \log^- \max\{|\lambda_j^n - 1|_\mu, |\det C_{n,k_i}(\lambda_i)|_\mu\}. \tag{3.15}$$

By Lemma 3.10, for every $i \in \mathcal{I}$ and $j \in \mathcal{L}$,

$$\sum_{\mu\in M_0} \log^- \max\{|\lambda_j^n - 1|_\mu, |\det C_{n,k_i}(\lambda_i)|_\mu\} = O(\log n), \tag{3.16}$$

for every $n \in \mathbb{N}$ sufficiently large. Putting together equations (3.15) and (3.16) we have, for every $\epsilon > 0$,

$$\log \gcd(\Omega_0, \Omega_{t+1}) \leq \epsilon n,$$

for n sufficiently large.
Observe now that

$$\log \gcd(\Omega_0, \Omega_{t+2}) \leq \sum_{i\in\mathcal{L}} \sum_{j\in\mathcal{K}} \sum_{\mu\in M_0} \log^- \max\{|\lambda_i^n - 1|_\mu, |\eta_j^n - 1|_\mu\}.$$

Following [4], we can now apply Proposition 1.13 (recall that our definition of $\log^-$ differs from that of [6], where $\log^- x = \min\{0, \log x\}$). We apply this proposition with $u = \lambda_i^n$ and $v = \eta_j^n$. Since $\lambda_i \nsim \eta_j$ for each $i \in \mathcal{L}$ and $j \in \mathcal{K}$, then for each $\tilde{\epsilon} > 0$

$$\sum_{\mu\in M_0} \log^- \max\{|\lambda_i^n - 1|_\mu, |\eta_j^n - 1|_\mu\} \leq \tilde{\epsilon} \max\{h(\lambda_i^n), h(\eta_j^n)\} = \tilde{\epsilon} n \max\{h(\lambda_i), h(\eta_j)\},$$

for n sufficiently large, for every $i \in \mathcal{L}$ and $j \in \mathcal{K}$. Therefore we get

$$\log \gcd(\Omega_0, \Omega_{t+2}) \leq \tilde{\epsilon} n \sum_{i\in\mathcal{L}} \sum_{j\in\mathcal{K}} \max\{h(\lambda_i), h(\eta_j)\}$$

and taking $\tilde{\epsilon} = \epsilon \left(\sum_{i \in \mathcal{L}} \sum_{j \in \mathcal{K}} \max\{h(\lambda_i), h(\eta_j)\} \right)^{-1}$, we obtain

$$\log \gcd (\Omega_0, \Omega_{t+2}) \leq \epsilon n,$$

for n sufficiently large.
We can now proceed by induction on t. If $t = 1$, i.e. if $h_{\gamma_1} \geq r + 1$ the proof of case 1 can be concluded since

$$\log \gcd_i(y_{n,r+1,i}) \leq \log \gcd (\Omega_0, \Omega_{t+1}) + \log \gcd (\Omega_0, \Omega_{t+2}) \leq \epsilon n + \epsilon n,$$

for n sufficiently large.
Otherwise, if $t > 1$, then $h_{\gamma_1} < r + 1$ and we are left with giving a suitable upper bound for

$$\log \gcd (\Omega_1, \Omega_2, \ldots, \Omega_t) .$$

Observe that $\Omega_1, \Omega_2, \ldots, \Omega_t$ are all the minors of order $r+1-h_{\gamma_1}$ of the matrix $B^n - I$, deprived of its blocks relative to eigenvalues in γ_1, that do not contain elements $\lambda^n - 1$ with $\lambda \in \Lambda^*$. For every $\gamma \neq \gamma_1$ we have $d - l - h_{\gamma_1} - h_\gamma + \bar{l} + \bar{h}_\gamma \geq r + 1 - h_{\gamma_1}$, then we can repeat the procedure up to here developed, by replacing d with $d - h_{\gamma_1}$, Γ with $\Gamma \setminus \{\gamma_1\}$, r with $r - h_{\gamma_1}$ and considering only the minors $\Omega_1, \Omega_2, \ldots, \Omega_t$ instead of all the minors of $B^n - I$. We come up with a new set $\{\Omega_0^1, \Omega_1^1, \ldots, \Omega_{t_1+2}^1\}$, where $t_1 < t$ and by the inductive hypothesis we can conclude that for every $\epsilon > 0$

$$\log \gcd_i(y_{n,r+1,i}) \leq \epsilon n$$

for n sufficiently large. Thus A is r-regular.
Case 2) Suppose now that there exists a $\gamma \in \Gamma$, say γ_1, such that $l - \bar{l} + h_{\gamma_1} - \bar{h}_{\gamma_1} \geq d - r$. This inequality is equivalent to $d - l - h_{\gamma_1} + \bar{l} + \bar{h}_{\gamma_1} < r + 1$ and this in turn amounts to say that in the determinant of each minor of order $r + 1$ of the matrix $B^n - I$ there is a factor $\lambda^n - 1$ with $\lambda \in \gamma_1 \cup \Lambda^*$.
Let now T be the order of torsion in the subgroup of $\mathbb{K}^*$ generated by the eigenvalues of B and observe that for each $\lambda_i \in \gamma_1$ there exist two integer a_i, b_i such that $\lambda_1^{a_i} = \lambda_i^{b_i}$. Let m be the least common multiple of T and the b_i's and consider the subset $\mathcal{N}$ of the natural numbers defined by

$$\mathcal{N} = \{n \in \mathbb{N} \text{ such that } n \equiv 0 \pmod{m}\}$$

For each $n \in \mathcal{N}$, say $n = jm$ with $j \in \mathbb{N}$ and for each $\mu \in M_0$ we have

$$\max_i \{ \left| y_{n,r+1,i} \right|_\mu \} \leq \left| \lambda_1^j - 1 \right|_\mu$$

and hence

$$\log \gcd_i(y_{n,r+1,i}) \geq \sum_{\mu \in M_0} \log^- \left| \lambda_1^j - 1 \right|_\mu$$

for every $j \in \mathbb{N}$. We will now prove that there exits $\rho > 0$ such that

$$\sum_{\mu \in M_0} \log^- \left|\lambda_1^j - 1\right|_\mu > \rho j \tag{3.17}$$

for every j in an infinite subset of $\mathcal{N}$. Observe that

$$\begin{aligned}
\sum_{\mu \in M_0} \log^- \left|\lambda_1^j - 1\right|_\mu &= \sum_{\mu \in M} \log^- \left|\lambda_1^j - 1\right|_\mu - \sum_{\mu \in M \setminus M_0} \log^- \left|\lambda_1^j - 1\right|_\mu \\
&= h\left(\lambda_1^j - 1\right) - \sum_{\mu \in M \setminus M_0} \log^- \left|\lambda_1^j - 1\right|_\mu \\
&= jh(\lambda_1) + O(1) - \sum_{\mu \in M \setminus M_0} \log^- \left|\lambda_1^j - 1\right|_\mu
\end{aligned}$$

Hence proving (3.17) amounts to prove that there exists $\rho > 0$ such that

$$\sum_{\mu \in M \setminus M_0} \log^- \left|\lambda_1^j - 1\right|_\mu < j\left(h(\lambda_1) - \rho\right) \tag{3.18}$$

for every j in an infinite subset of $\mathcal{N}$. The last inequality is true since we will now prove that for all$\epsilon > 0$

$$\sum_{\mu \in M \setminus M_0} \log^- \left|\lambda_1^j - 1\right|_\mu < \epsilon j + O(1) \tag{3.19}$$

for every j in an infinite subset of $\mathcal{N}$, by applying the (generalized) Roth's theorem [1, chapter 6] in the following form.

Theorem 3.11 (Roth). *Let $\mathbb{K}$ be a number field and S a finite set of places. For each $\mu \in S$ let α_μ be $\mathbb{K}-$algebraic. Then for each $\epsilon > 0$, there exist only finitely many $\beta \in \mathbb{K}$ such that*

$$\prod_{\mu \in S} \min\left(1, |\beta - \alpha_\mu|_\mu\right) \leq H(\beta)^{-2-\epsilon}$$

To prove (3.19), let us define

$$\begin{aligned}
D(j) &:= \prod_{\substack{\mu \in M \setminus M_0 \\ |\lambda_1|_\mu < 1}} \min\left\{1, \left|\lambda_1^j - 1\right|_\mu\right\} \\
E(j) &:= \prod_{\substack{\mu \in M \setminus M_0 \\ |\lambda_1|_\mu > 1}} \min\left\{1, \left|\lambda_1^j - \infty\right|_\mu\right\} \\
F(j) &:= \prod_{\substack{\mu \in M_0 \\ |\lambda_1|_\mu < 1}} \min\left\{1, \left|\lambda_1^j - 0\right|_\mu\right\},
\end{aligned}$$

where $\left|\lambda_1^j - \infty\right|_\mu := \left|\lambda_1^j\right|_\mu^{-1}$. Since the products in $D(j), E(j), F(j)$ are over a finite set of places, then Lang's generalization 1.7 of Roth's theorem implies that, for every $\epsilon_1 > 0$,

$$D(j)E(j)F(j) > H\left(\lambda_1^j\right)^{-2-\epsilon_1}$$

for every j sufficiently large. Observe now that

$$E(j) = \prod_{\substack{\mu\in M\setminus M_0\\ |\lambda_1|_\mu>1}} \frac{1}{\max\left\{1, \left|\lambda_1^j\right|_\mu\right\}} = H(\lambda_1^j)^{-1}$$

since λ_1 is an algebraic integer. Moreover

$$F(j) = \prod_{\substack{\mu\in M_0\\ |\lambda_1|_\mu<1}} \left|\lambda_1^j\right|_\mu = \prod_{\mu\in M_0} \left|\lambda_1^j\right|_\mu = \prod_{\mu\in M\setminus M_0} \left|\lambda_1^j\right|_\mu^{-1} = c^j H(\lambda_1^j)^{-1}$$

where

$$c := \prod_{\substack{\mu\in M\setminus M_0\\ |\lambda_1|_\mu<1}} |\lambda_1|^{-1}$$

is a constant, depending on λ_1, with $c > 1$. Hence, putting everything together,

$$D(j) > c^{-j} H(\lambda_1)^{-j\epsilon_1}$$

for every j sufficiently large. Let us now define $b := c^{1/\epsilon_1}$ and observe that for every $\delta > 1$ and for every $\epsilon > 0$,

$$c^{-j} H(\lambda_1)^{-j\epsilon_1} > \delta \exp(-j\epsilon)$$

for every j sufficiently large, when

$$\epsilon_1 < \frac{\epsilon}{\log\left(bH(\lambda_1)\right)}$$

Hence, taking into account that

$$\sum_{\mu\in M\setminus M_0} \log^- \left|\lambda_1^j - 1\right|_\mu = \log \prod_{\mu\in M\setminus M_0} \min\left\{1, \left|\lambda_1^j - 1\right|_\mu\right\}^{-1} = \log D(j)^{-1}$$

for every j sufficiently large, we conclude that

$$\sum_{\mu\in M\setminus M_0} \log^- \left|\lambda_1^j - 1\right|_\mu < \log\left(\delta^{-1}\exp(j\epsilon)\right) = j\epsilon + O(1)$$

for every j sufficiently large and this proves (3.19).
We can therefore conclude that

$$\begin{aligned}\log \gcd_i(y_{n,r+1,i}) &\geq \sum_{\mu\in M_0} \log^- \left|\lambda_1^j - 1\right|_\mu \\ &= jh(\lambda_1) + O(1) - \sum_{\mu\in M\setminus M_0} \log^- \left|\lambda_1^j - 1\right|_\mu \\ &> jh(\lambda_1) - j\epsilon + O(1) \\ &= j(h(\lambda_1) - \epsilon) + O(1) > \rho j\end{aligned}$$

for j sufficiently large, where ρ is for instance $(h(\lambda_1) - \epsilon)/2$. This proves (3.17) and then A is r-exceptional. □

Proof of Corollary 3.7. If A is r-exceptional, then by Theorem 3.4, there exists $\gamma \in \Gamma$ such that $l + h_\gamma \geq d - r + \bar{l} + \overline{h}_\gamma$.
If A is diagonalizable, i.e. if $f = 0$, then $\bar{l} + \overline{h}_\gamma = 0$ and hence $l + h_\gamma \geq d - r$. Thus $e \leq d - (l + h_\gamma) + 1 \leq d - (d - r) + 1 = r + 1$.
If A is not diagonalizable, i.e. if $f = 1$, then $\bar{l} + \overline{h}_\gamma \geq 1$ and hence $l + h_\gamma \geq d - r + 1$. Thus $e \leq d - (l + h_\gamma) + 1 \leq d - (d - r + 1) + 1 = r$.
In both cases A r-exceptional implies $e + f \leq r + 1$. □

Let us now come to the proof of Theorem 3.8.

Proof of Theorem 3.8. Let ϕ be an endomorphism of a free module over a finitely generated ring R of characteristic zero and let d be the dimension of the module. Let $\lambda_1, \lambda_2, \ldots, \lambda_d$ be the eigenvalues of ϕ each repeated with its algebraic multiplicity. Finally let $\alpha_{n,1}, \alpha_{n,2}, \ldots, \alpha_{n,d}$ be the invariants of $\phi^n - I$, that are rational integers by hypothesis. Recalling that

$$\begin{aligned}\alpha_{n,1} &= s_1(\lambda_1^n - 1, \ldots, \lambda_d^n - 1) \\ \alpha_{n,2} &= s_2(\lambda_1^n - 1, \ldots, \lambda_d^n - 1) \\ &\vdots \quad\quad \vdots \\ \alpha_{n,d} &= s_d(\lambda_1^n - 1, \ldots, \lambda_d^n - 1)\end{aligned}$$

where s_k is the k-th elementary symmetric polynomial, we have

$$(\lambda_i^n - 1)^d = \sum_{k=1}^{d} (-1)^{k+1} (\lambda_i^n - 1)^{d-k} \alpha_{n,k} \tag{3.20}$$

for every $i = 1, 2, \ldots, d$. Fix now a positive integer N and suppose that $N|\alpha_{n,k}^{d!k^{-1}}$ for every $k = 1, \ldots, d$. Then $N|\alpha_{n,k}^{d!}$ for every $k = 1, \ldots, d$, and using (3.20), we have

$$\begin{aligned}
\log \gcd_i(\lambda_i^n - 1)^d &= \sum_{\mu \in M_0} \log^- \max_i \left|(\lambda_i^n - 1)^d\right|_\mu \\
&= \sum_{\mu \in M_0} \log^- \max_i \left|\sum_{k=1}^{d} (-1)^{k+1} (\lambda_i^n - 1)^{d-k} \alpha_{n,k}\right|_\mu \\
&\geq \sum_{\mu \in M_0} \log^- \max_i \max_k \left|(\lambda_i^n - 1)^{d-k} \alpha_{n,k}\right|_\mu \\
&\geq \sum_{\mu \in M_0} \log^- \max_k \left|\alpha_{n,k}\right|_\mu = \log \gcd_k(\alpha_{n,k}) \geq d!^{-1} \log N
\end{aligned}$$

where M_0 is the set of non archimedean valuations of the field of fractions of the ring R. Suppose now that λ_1 and λ_2 are two multiplicatively independent eigenvalues of ϕ and apply Proposition 1.13, as we did in proving Theorem 3.4. We obtain, for every $\epsilon > 0$,

$$\log \gcd_i(\lambda_i^n - 1) \leq \log \gcd \{\lambda_1^n - 1, \lambda_2^n - 1\} \leq \epsilon n \tag{3.21}$$

for every n sufficiently large. Therefore

$$\log N \leq d! d \epsilon n$$

for every n sufficiently large, i.e.

$$\lim_{N \to \infty} \frac{k(\phi, N)}{\log N} = +\infty$$

On the other hand if all the eigenvalues of ϕ are pairwise multiplicatively dependent, we can proceed as in the proof of Theorem 3.4. For every $i = 1, \ldots, d$ there exist two integers a_i, b_i, not both zero, such that $\lambda_1^{a_i} = \lambda_i^{b_i}$. Let m be the least common multiple of the b_i's and consider the subset $\mathcal{N}$ of the natural numbers defined by

$$\mathcal{N} = \{n \in \mathbb{N} \text{ such that } n \equiv 0 \pmod{m}\}$$

For each $n \in \mathcal{N}$, say $n = jm$ with $j \in \mathbb{N}$ and for each $\mu \in M_0$ we have

$$\max_k \{\left|\alpha_{n,k}\right|_\mu\} \leq \left|\lambda_1^j - 1\right|_\mu$$

and applying the Roth's theorem as in the proof of Theorem 3.4 we get, for every $\epsilon > 0$,

$$\begin{aligned}
\log \gcd_k(\alpha_{n,k}^{d!k^{-1}}) &\geq \log \gcd_k(\alpha_{n,k}) \\
&\geq \sum_{\mu \in M_0} \log^- \left|\lambda_1^j - 1\right|_\mu > j(1 - \epsilon) h(\lambda_1) + O(1)
\end{aligned}$$

for j sufficiently large. Hence there exists a positive constant ρ such that

$$\log \gcd_k(\alpha_{n,k}^{d!k^{-1}}) > \rho n$$

for every sufficiently large $n \in \mathcal{N}$. Then, taking $N_n := \gcd_k(\alpha_{n,k}^{d!k^{-1}})$, we get

$$k(\phi, N_n) \leq n \leq \frac{1}{\rho} \log \gcd_k(\alpha_{n,k}^{d!k^{-1}}) = \frac{1}{\rho} \log N_n$$

and so

$$\frac{k(\phi, N_n)}{\log N_n} \leq \frac{1}{\rho}, \quad \forall n \in \mathcal{N}.$$

□

Chapter 4

Rational points on elliptic curves

4.1 On the exponent of the group of rational points

As an application of Theorem 3.8 we can recover a result of Luca and Shparlinski, presented in [13], on the exponent of the group of rational points on an elliptic curve defined over a finite field. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, with q elements, and let $E(\mathbb{F}_{q^n})$ be the group of $\mathbb{F}_{q^n}-$rational points. We have seen in proposition 2.11 that $E(\mathbb{F}_{q^n})$ has the following structure:

$$E(\mathbb{F}_{q^n}) \cong (\mathbb{Z}/m(q^n)\mathbb{Z}) \times (\mathbb{Z}/l(q^n)\mathbb{Z}) \tag{4.1}$$

where $m(q^n), l(q^n)$ are uniquely determined integers such that $m(q^n)|l(q^n)$. The integer $l(q^n)$ is the largest possible order of torsion of an $\mathbb{F}_{q^n}-$rational point and it is called the *exponent* of $E(\mathbb{F}_{q^n})$. Moreover the Hasse-Weil relation for the cardinality $\sharp E(\mathbb{F}_{q^n})$ of the set of $\mathbb{F}_{q^n}-$rational points is

$$\sharp E(\mathbb{F}_{q^n}) = q^n + 1 - \mathrm{Tr}(\phi^n) \tag{4.2}$$

where ϕ is the Frobenius isogeny of E and $\mathrm{Tr}(\phi^n)$ is the trace of its n-th power. Using equation (4.2) and the fact that the eigenvalues α, β of ϕ are complex conjugates with $|\alpha| = |\beta| = q^{1/2}$, it is immediate to obtain the bound

$$l(q^n) \geq q^{n/2} - 1 \tag{4.3}$$

for every n. In fact, since $m(q^n)|l(q^n)$, we have

$$\begin{aligned} l(q^n) &\geq (l(q^n)m(q^n))^{1/2} = \left(\sharp E(\mathbb{F}_{q^n})\right)^{1/2} \\ &= (q^n + 1 - \mathrm{Tr}(\phi^n))^{1/2} \geq \left(q^n + 1 - 2q^{n/2}\right)^{1/2} \\ &= q^{n/2} - 1 \end{aligned}$$

We will apply Theorem 3.8 to recover the much stronger lower bound of Luca and Shparlinski for the exponent of $E(\mathbb{F}_{q^n})$ for an ordinary elliptic curve. To state their theorem, recall that an elliptic curve defined over $\mathbb{F}_q$, with $q = p^k$, is called ordinary if the group of p-torsion points is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and supersingular if 0 is the unique p-torsion point.

Lemma 4.1. *An ordinary elliptic curve E possesses two multiplicatively independent eigenvalues.*

Proof. Let ϕ be the Frobenius endomorphism of the elliptic curve E and let α and β be its eigenvalues. If α, β were multiplicatively dependent, then $\alpha^a = \beta^b$, for suitable $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ and this would imply $a = b$, since $|\alpha| = |\beta| = \sqrt{q}$. Then $\alpha^{2a} + \beta^{2a} \equiv 0 \pmod{q^a}$ and E would be supersingular, contradicting the hypothesis. □

Theorem 4.2 (F. Luca and E. Shparlinski)**.** *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then for every $\epsilon > 0$,*

$$l(q^n) \geq q^{n(1-\epsilon)} \quad \textit{for every } n \textit{ sufficiently large}$$

if and only if E is ordinary.

Luca and Shparlinski provide moreover an upper bound for the number of exceptional values of n, but, since their proof relies on Schmidt's subspace theorem, which is non effective, they cannot find explicitly the exceptional values, i.e. they cannot find an upper bound for the largest exceptional value of n. Before proving Theorem 4.2, let us mention that an analogue of this theorem was proved by Schoof in [15], in the following context: let E be an elliptic curve defined over $\mathbb{Q}$, without complex multiplication and let $l(p)$ be the exponent of the group $E(\mathbb{F}_p)$, for the primes p of good reduction. Schoof studies the exponent $l(p)$, for a given elliptic curve, as p varies over the primes of good reduction and proves that

$$l(p) \geq C_E \frac{p^{1/2} \log p}{\log \log p},$$

where C_E is a positive constant, depending only on E.

To prove Theorem 4.2, we will apply Theorem 3.8 with ϕ equals to the Frobenius endomorphism of the elliptic curve E, by showing, in the following lemma, that $m(q^n)$, in the notation of (4.1), divides both $\det(\phi^n - I)$ and $(\mathrm{Tr}(\phi^n - I))^2$. This fact, together with the Hasse-Weil relation (4.2), will provide the desired result.

Lemma 4.3. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with characteristic p and let*

$$E(\mathbb{F}_q) \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/l\mathbb{Z})$$

be the decomposition of the group of rational points with $m, l \geq 1$ and $m|l$. Let ϕ be the Frobenius endomorphism for E, acting on the Tate module for some prime distinct from p. Then we have

$$m|\det(\phi - I), \qquad m|Tr(\phi - I). \tag{4.4}$$

Proof. Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and let $\phi : E \to E$ be the Frobenius endomorphism. Let m, l be the positive integers that determine the structure of the group of $\mathbb{F}_q$-rational points, as in (4.1), with $m|l$. Recall now that we may define the determinant and the trace of an endomorphism ψ of an elliptic curve E by choosing a prime w different from the characteristic of $\mathbb{F}_q$ and considering the representation

$$\begin{aligned} \mathrm{End}(E) &\to \mathrm{End}(T_w(E)) \\ \phi &\to \phi_w \end{aligned}$$

of the ring $\mathrm{End}(E)$ of endomorphisms of E into the ring of endomorphisms of the w-adic Tate module of E. Since w is coprime with q, then $T_w(E)$ is isomorphic to $\mathbb{Z}_w \times \mathbb{Z}_w$ and if we choose a basis for this $\mathbb{Z}_w$-module, we can write ψ_w as a 2×2 matrix whose entries belong to $\mathbb{Z}_w$. It is then possible to compute $\det(\psi_w)$ and $\mathrm{Tr}(\psi_w)$, and it turns out that these quantities are rational integers independent from the chosen prime w [16, chapter 5]. We can then define

$$\begin{aligned} \det(\psi) &:= \det(\psi_w) \\ \mathrm{Tr}(\psi) &:= \mathrm{Tr}(\psi_w) \end{aligned}$$

Observe now that m-torsion points are $\mathbb{F}_q$-rational: it is obvious, from the structure of $E(\mathbb{F}_q)$, that there are at least m^2 rational points of order m, and by Proposition 2.5, there can not be any more of them. This implies that m is coprime with q (because otherwise there would be less than m^2 points of order m, again by Proposition 2.5) and that the Frobenius ϕ acts trivially on $E[m]$. Since this action is compatible with that on Tate modules $T_w(E)$, for each prime w dividing m, it follows that ϕ reduced modulo m is the identity matrix in $\mathrm{Aut}(E[m])$. This implies that

$$m|\det(\phi - I)$$

and

$$m|\mathrm{Tr}\,(\phi - I)$$

□

We would like to remark that the arguments used in the proof of Lemma 4.3 are quite standard.

Proof of Theorem 4.2. Let now $m(q^n)$ and $l(q^n)$ be the positive integers of the decomposition

$$E(\mathbb{F}_{q^n}) \cong (\mathbb{Z}/m(q^n)\mathbb{Z}) \times (\mathbb{Z}/l(q^n)\mathbb{Z}) .$$

By the preceeding lemma it follows that

$$m(q^n)|\det(\phi^n - I) \tag{4.5}$$

and

$$m(q^n)|\mathrm{Tr}\,(\phi^n - I)$$

and then

$$m(q^n)|\,(\mathrm{Tr}(\phi^n - I))^2 \tag{4.6}$$

If E is an ordinary elliptic curve, then, by Lemma 4.1, the eigenvalues α, β of the Frobenius endomorphism are multiplicatively independent. We can then apply Theorem 3.8: since (4.5) and (4.6) hold and the only invariants of the Frobenius are the determinant and the trace, then

$$k(\phi, m(q^n)) \leq n.$$

It follows that

$$\frac{n}{\log m(q^n)} \geq \frac{k(\phi, m(q^n))}{\log m(q^n)}$$

and therefore

$$\lim_{n\to\infty} \frac{n}{\log m(q^n)} = +\infty \tag{4.7}$$

But recalling the Hasse-Weil relation (4.2)

$$\sharp E(\mathbb{F}_{q^n}) = l(q^n)m(q^n) = q^n + O(q^{n/2}),$$

we get

$$\lim_{n\to\infty} \frac{\log l(q^n) + \log m(q^n)}{n \log q} = 1$$

Hence (4.7) implies

$$\lim_{n\to\infty} \frac{\log l(q^n)}{n \log q} = 1$$

and this in turn implies that for every $\epsilon > 0$,

$$l(q^n) > q^{n(1-\epsilon)}$$

for every n sufficiently large.

On the other hand if E is supersingular, there exist [11, chapter 13] two strictly positive integers a, b such that $\phi^a = [p^b]$, where $p = \mathrm{char}(\mathbb{F}_q)$. Let $\mathcal{N} \coloneqq \{n \in \mathbb{N} | n \equiv$

0 (mod a)} and observe that if $n \in \mathcal{N}$, say $n = ja$, with $j \in \mathbb{N}$, then $P \in E$ is $\mathbb{F}_{q^n}-$rational if and only if

$$0 = (\phi^n - I)(P) = [p^{bj} - 1](P)$$

i.e. if and only if P is a $(p^{bj} - 1)-$torsion point. But

$$E[p^{bj} - 1] \cong \mathbb{Z}/(p^{bj} - 1)\mathbb{Z} \times \mathbb{Z}/(p^{bj} - 1)\mathbb{Z}$$

because $p^{bj} - 1$ is coprime with p. Hence

$$m(q^n) = p^{b\frac{n}{a}} - 1$$

for every $n \in \mathcal{N}$. If for all$\epsilon > 0$, $l(q^n) > q^{n(1-\epsilon)}$ for every n sufficiently large, then

$$\sharp E(\mathbb{F}_{q^n}) = l(q^n)m(q^n) > q^{n(1-\epsilon)}\left(p^{b\frac{n}{a}} - 1\right) \tag{4.8}$$

for every $n \in \mathcal{N}$ sufficiently large and this would contradict equation (2.11), that we recall here for the reader's convenience:

$$\sharp E(\mathbb{F}_{q^n}) < 2q^n + 1,$$

for every $n \in \mathbb{N}$. This bound, together with (4.8), would imply

$$q^{n(1-\epsilon)}\left(p^{b\frac{n}{a}} - 1\right) < 2q^n + 1$$

for every $n \in \mathcal{N}$ sufficiently large, leading to a contradiction when ϵ is sufficiently small. □

4.2 Isogenies characterization

Consider now two ordinary elliptic curves E_1 and E_2 defined over $\mathbb{F}_q$. Let $\mathcal{A} := E_1 \times E_2$ be their product and let $\mathcal{A}(\mathbb{F}_{q^n}) = E_1(\mathbb{F}_{q^n}) \times E_2(\mathbb{F}_{q^n})$ be the group of its $\mathbb{F}_{q^n}-$rational points. Since

$$E_i(\mathbb{F}_{q^n}) \cong (\mathbb{Z}/m_i(q^n)\mathbb{Z}) \times (\mathbb{Z}/l_i(q^n)\mathbb{Z})$$

for $i = 1, 2$, then

$$\mathcal{A}(\mathbb{F}_{q^n}) \cong (\mathbb{Z}/m_1(q^n)\mathbb{Z}) \times (\mathbb{Z}/l_1(q^n)\mathbb{Z}) \times (\mathbb{Z}/m_2(q^n)\mathbb{Z}) \times (\mathbb{Z}/l_2(q^n)\mathbb{Z})$$

and then

$$\mathcal{A}(\mathbb{F}_{q^n}) \cong (\mathbb{Z}/l(q^n)\mathbb{Z}) \times M(q^n)$$

where

$$l(q^n) := \mathrm{lcm}(l_1(q^n), l_2(q^n))$$

is the least common multiple of the exponents of the groups $E_1(\mathbb{F}_{q^n})$ and $E_2(\mathbb{F}_{q^n})$ and $M(q^n)$ is a finite, not necessarily cyclic, group. We will apply Theorems 3.4 and 4.2 to prove the following necessary and sufficient condition on the structure of $\mathcal{A}(\mathbb{F}_{q^n})$ for the two curves to be isogenous.

Theorem 4.4. *Let E_1 and E_2 be two ordinary elliptic curves over a finite field $\mathbb{F}_q$. Then for every $\epsilon > 0$,*

$$l(q^n) \geq q^{2n(1-\epsilon)} \quad \textit{for every } n \textit{ sufficiently large} \tag{4.9}$$

if and only if E_1 and E_2 are not isogenous over $\overline{\mathbb{F}}_q$. Hence if E_1 and E_2 are not isogenous then

$$\gcd\left(\sharp E_1(\mathbb{F}_{q^n}), \sharp E_2(\mathbb{F}_{q^n})\right) < \exp(\epsilon n) \quad \textit{for every } n \textit{ sufficiently large.} \tag{4.10}$$

Equation (4.10) can be paraphrased by saying that the groups of $\mathbb{F}_{q^n}-$rational points of two ordinary non isogenous elliptic curves have orders which tend to be coprime as n approaches infinity.

To prove Theorem 4.4, recall that two elliptic curves E_1 and E_2 are isogenous over $\mathbb{F}_q$ if and only if they have the same number of $\mathbb{F}_q-$rational points [16, chapter 5]. So if E_1 and E_2 are two $\mathbb{F}_q-$isogenous elliptic curves, then the Frobenius endomorphisms ϕ_1 and ϕ_2 have the same characteristic polynomial and hence ϕ_1 and ϕ_2 have the same eigenvalues.
Viceversa let $\alpha_i, \overline{\alpha}_i$ be the complex conjugate eigenvalues of the Frobenius endomorphism of E_i, for $i = 1, 2$. If ϕ_1 and ϕ_2 have multiplicatively dependent eigenvalues, then there exists a positive integer a such that $\alpha_1^a = \alpha_2^a$ and then automatically $\overline{\alpha}_1^a = \overline{\alpha}_2^a$. Hence ϕ_1^a and ϕ_2^a have the same eigenvalues and therefore the same characteristic polynomial. Then $\sharp E_1(\mathbb{F}_{q^a}) = \sharp E_2(\mathbb{F}_{q^a})$ and so E_1 and E_2 are isogenous over $\mathbb{F}_{q^a}$. Observe moreover that $\alpha_1^a = \alpha_2^a$ implies $\alpha_1 = \zeta\alpha_2$ for a certain $a-$th root of unity ζ which belongs to $\mathbb{Q}(\alpha_1, \alpha_2)$. Hence $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 1, 2$ or 4. If $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 1$ then $\zeta = \pm 1$ and $a = 1$ or 2; if $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$ then $\zeta = \pm\imath, \pm\rho, \pm\rho^2$, where $\rho = \exp(2\pi\imath/3)$ and $a = 3, 4$ or 6; if $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ then ζ is a primitive root of unity of order 5, 8, 10 or 12 and consequently $a = 5, 8, 10$ or 12. To summarize, if ϕ_1 and ϕ_2 have multiplicatively dependent eigenvalues, then E_1 and E_2 are isogenous over $\mathbb{F}_{q^a}$, where $a \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$.

Proof of Theorem 4.4. Since E_1 and E_2 are ordinary, by Theorem 4.2 we have, for all $\epsilon > 0$,

$$l_1(q^n)l_2(q^n) \geq q^{2n(1-\epsilon)} \tag{4.11}$$

for every n sufficiently large. Let ϕ_1 and ϕ_2 be the Frobenius isogenies of E_1 and E_2 and let ϕ be the Frobenius isogeny of their product $\mathcal{A}$. We can choose a basis in $T_l(\mathcal{A})$ such that the matrix representing ϕ is diagonal of the form

$$\phi_l \coloneqq \begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \overline{\alpha}_1 & 0 & 0 \\ 0 & 0 & \alpha_2 & 0 \\ 0 & 0 & 0 & \overline{\alpha}_2 \end{pmatrix} \tag{4.12}$$

where $\alpha_i, \overline{\alpha}_i$ are the complex conjugate eigenvalues of ϕ_i, $i = 1, 2$. If E_1 and E_2 are not $\mathbb{F}_q-$isogenous, then by the remark preceding this proof and the fact that E_1 and E_2 are ordinary, $\alpha_1, \overline{\alpha}_1, \alpha_2, \overline{\alpha}_2$ are pairwise multiplicative independent. Hence, by Theorem 3.4 the matrix (4.12) representing ϕ_l is $2-$regular, in the sense that (3.10) holds with $r = 2$. If we define $\Delta(q^n) \coloneqq \gcd(l_1(q^n), l_2(q^n))$, then $\Delta(q^n)$ divides all the determinants of the minors of order 3 of $\phi_l^n - I$ and then for all $\epsilon > 0$

$$\Delta(q^n) < \exp(\epsilon n) \quad \text{for } n \text{ sufficiently large.} \tag{4.13}$$

We can then conclude by (4.11) and (4.13) that for all $\epsilon > 0$

$$l(q^n) = \frac{l_1(q^n) l_2(q^n)}{\Delta(q^n)} > q^{2n(1-\epsilon)} \exp(-\epsilon n) > q^{2n(1-2\epsilon)} \quad \text{for } n \text{ sufficiently large}$$

and the assertion follows by redefining ϵ.

Conversely if E_1 and E_2 are $\mathbb{F}_q-$isogenous, then α_1 and α_2 are multiplicatively dependent (possibly exchanging α_2 with $\overline{\alpha}_2$). Then by Theorem 3.4 the matrix (4.12) is $2-$exceptional, i.e. $\exists \rho > 0$ and an infinite subset $\mathcal{N} \subset \mathbb{N}$ such that, if we let $l_i'(q^n) \coloneqq l_i(q^n)/\Delta(q^n)$ for $i = 1, 2$, then for all $\epsilon > 0$

$$\begin{aligned}
\rho n \;<\; & \log \gcd\big((\alpha_1^n - 1)(\overline{\alpha}_1^n - 1)(\alpha_2^n - 1), (\alpha_1^n - 1)(\overline{\alpha}_1^n - 1)(\overline{\alpha}_2^n - 1), \\
& (\alpha_1^n - 1)(\alpha_2^n - 1)(\overline{\alpha}_2^n - 1), (\overline{\alpha}_1^n - 1)(\alpha_2^n - 1)(\overline{\alpha}_2^n - 1)\big) \\
= \; & \log \gcd\big(l_1(q^n) m_1(q^n)(\alpha_2^n - 1), l_1(q^n) m_1(q^n)(\overline{\alpha}_2^n - 1), \\
& (\alpha_1^n - 1) l_2(q^n) m_2(q^n), (\overline{\alpha}_1^n - 1) l_2(q^n) m_2(q^n)\big) \\
= \; & \log \Delta(q^n) + \log \gcd\big(l_1'(q^n) m_1(q^n)(\alpha_2^n - 1), l_1'(q^n) m_1(q^n)(\overline{\alpha}_2^n - 1), \\
& (\alpha_1^n - 1) l_2'(q^n) m_2(q^n), (\overline{\alpha}_1^n - 1) l_2'(q^n) m_2(q^n)\big) \\
\leq \; & \log \Delta(q^n) + \log \gcd\big(\alpha_2^n - 1, \overline{\alpha}_2^n - 1\big) \\
& + \log \gcd\big(l_1'(q^n) m_1(q^n), (\alpha_1^n - 1) l_2'(q^n) m_2(q^n), (\overline{\alpha}_1^n - 1) l_2'(q^n) m_2(q^n)\big) \\
\leq \; & \log \Delta(q^n) + \log \gcd\big(\alpha_2^n - 1, \overline{\alpha}_2^n - 1\big) \\
& + \log \gcd\big(l_1'(q^n) m_1(q^n), l_2'(q^n) m_2(q^n)\big) + \log \gcd\big(\alpha_1^n - 1, \overline{\alpha}_1^n - 1\big) \\
= \; & \log \Delta(q^n) + \log \gcd\big(\alpha_2^n - 1, \overline{\alpha}_2^n - 1\big) \\
& + \log \gcd\big(m_1(q^n), m_2(q^n)\big) + \log \gcd\big(\alpha_1^n - 1, \overline{\alpha}_1^n - 1\big) \\
\leq \; & \log \Delta(q^n) + \epsilon n + \log m_1(q^n) + \epsilon n
\end{aligned}$$

for every $n \in \mathcal{N}$ sufficiently large, where the last inequality follows since α_i and $\overline{\alpha}_i$ are multiplicatively independent, for $i = 1$ and 2. Remember now that

$$m_1(q^n) < \exp(\epsilon n)$$

for n sufficiently large, since E_1 is ordinary. This proves that

$$\log \Delta(q^n) > \rho n - 3\epsilon n$$

for every $n \in \mathcal{N}$ sufficiently large. If $\rho' > 0$ is a real constant, $\rho' < \rho$, then

$$\Delta(q^n) > \exp(\rho' n)$$

for every $n \in \mathcal{N}$ sufficiently large. Hence

$$l(q^n) = \frac{l_1(q^n) l_2(q^n)}{\Delta(q^n)} < l_1(q^n) l_2(q^n) \exp(-\rho' n)$$

for every $n \in \mathcal{N}$ sufficiently large.
Moreover, recalling the upper bound (2.11), he have that

$$l_1(q^n) l_2(q^n) \leq \sharp E_1(\mathbb{F}_{q^n}) \sharp E_2(\mathbb{F}_{q^n}) < (2q^n + 1)^2 < 5q^{2n}$$

for n sufficiently large and so

$$l(q^n) =< 5q^{2n} \exp(-\rho' n)$$

for every $n \in \mathcal{N}$ sufficiently large and this contradicts (4.9) if

$$\epsilon < \frac{\rho'}{4 \log q}$$

It is now straightforward to prove (4.10). In fact, if E_1 and E_2 are ordinary and not isogenous, then (4.7) and (4.13) imply that for every $\epsilon > 0$

$$\begin{aligned} \gcd\left(\sharp E_1(\mathbb{F}_{q^n}), \sharp E_2(\mathbb{F}_{q^n})\right) &= \gcd\left(m_1(q^n) l_1(q^n), m_2(q^n) l_2(q^n)\right) \\ &\leq m_1(q^n) m_2(q^n) \Delta(q^n) \leq \exp\left(\frac{\epsilon}{3} n\right)^3 = \exp(\epsilon n) \end{aligned}$$

for every n sufficiently large. □

Bibliography

[1] E. Bombieri and W. Gubler. *Heights in diophantine geometry*, volume 4 of *New mathematical monographs*. Cambridge University Press, Cambridge, 2006.

[2] A. Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[3] Y. Bugeaud, P. Corvaja, and U. Zannier. An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. *Math. Z.*, 243(1):79–84, 2003.

[4] P. Corvaja, Z. Rudnick, and U. Zannier. A lower bound for periods of matrices. *Comm. Math. Phys.*, 252(1-3):535–541, 2004.

[5] P. Corvaja and U. Zannier. On the greatest prime factor of $(ab + 1)(ac + 1)$. *Proc. Amer. Math. Soc.*, 131(6):1705–1709 (electronic), 2003.

[6] P. Corvaja and U. Zannier. A lower bound for the height of a rational function at S-unit points. *Monatsh. Math.*, 144(3):203–224, 2005.

[7] J.-H. Evertse. An improvement of the quantitative subspace theorem. *Compositio Math.*, 101(3):225–311, 1996.

[8] J.-H. Evertse and H. P. Schlickewei. A quantitative version of the absolute subspace theorem. *J. reine angew. Math.*, 548:21–127, 2002.

[9] M. Hindry and J. H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[10] J. E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.

[11] D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[12] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[13] F. Luca and I. E. Shparlinski. On the exponent of the group of points on elliptic curves in extension fields. *Int. Math. Res. Not.*, (23):1391–1409, 2005.

[14] W. M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[15] R. Schoof. The exponents of the groups of points on the reductions of an elliptic curve. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 325–335. Birkhäuser Boston, Boston, MA, 1991.

[16] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[17] U. Zannier. *Some applications of diophantine approximation to diophantine equations*. Forum, Editrice Universitaria Udinese srl, Udine, Italy, first edition, 2003.