Multiplicative and additive relations for values of rational functions and points on elliptic curves

Alina Ostafe

The University of New South Wales

Goal of the talk

Motivating question:

Let E be an elliptic curve over $\mathbb{Q}$ and let $\varphi_1, \dots, \varphi_s, \varrho_1, \dots, \varrho_n \in \mathbb{Q}(X)$ such that $\varphi_1, \dots, \varphi_s$ are multiplicatively independent and the points $(\varrho_1(X), \cdot), \dots, (\varrho_n(X), \cdot)$ in $E(\overline{\mathbb{Q}(X)})$ are linearly independent over $\mathbb{Z}$.

Describe the set of elements $\alpha \in \overline{\mathbb{Q}}$ such that:

- *the values $\varphi_1(\alpha), \dots, \varphi_s(\alpha)$ remain* **multiplicatively independent**, *or*
- *the points $(\varphi_1(\alpha), \cdot), \dots, (\varphi_s(\alpha), \cdot)$ in $E(\overline{\mathbb{Q}})$ are* **linearly independent**.

We present various finiteness results for multiplicative and additive relations as above, both in $\overline{\mathbb{Q}}$ (or in other "interesting" subfields) and also in $\overline{\mathbb{F}}_p$.

Multiplicative dependence among values of rational functions

Notation and set-up

- $\mathbb{U}$: the set of all roots of unity in $\overline{\mathbb{Q}}$;
- $\mathbb{K}$: number field;
- $\mathbb{K}^c = \mathbb{K}(\mathbb{U})$: the cyclotomic closure of $\mathbb{K}$;
- $\varphi_1, \ldots, \varphi_m \in \mathbb{K}(X)$;
- for $\alpha \in \mathbb{K}$, $\mathrm{h}(\alpha) =$ the absolute logarithmic Weil height of α:

$$\mathrm{h}(\alpha) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} n_v \max\{0, \log |\alpha|_v\}, \ n_v = [\mathbb{K}_v : \mathbb{Q}_v]$$

Definition

- $\varphi_1, \ldots, \varphi_m \in \mathbb{K}(X)$ are *multiplicatively independent (mult. indep.) with constants* if there exists no $(\nu_1, \ldots, \nu_m) \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$ such that

$$\varphi_1^{\nu_1} \cdots \varphi_m^{\nu_m} = a \in \mathbb{K}^*.$$

- If we only allow $a = 1$, we say that $\varphi_1, \ldots, \varphi_m$ are mult. indep.

Let

$$\mathcal{S} = \{\alpha \in \overline{\mathbb{Q}} : \varphi_1(\alpha), \ldots, \varphi_m(\alpha) \text{ are mult. dep.}\}.$$

Goal: **finiteness** of the set $\mathcal{S}$, unless the functions $\varphi_1, \ldots, \varphi_m$ are special.

If $\varphi_1, \ldots, \varphi_m$ are mult. dep. $\Longrightarrow$ a fixed dependence occurs for all points $\alpha \in \overline{\mathbb{Q}}$. Thus, our main assumption will be

$\varphi_1, \ldots, \varphi_m$ **are mult. indep.**

Torsion points on plane curves

torsion points = coordinates roots of unity.

The following result was conjectured by *Lang* and proved by *Ihara, Serre & Tate* (*1960s*):

Informally:

The intersection of an irreducible curve $\mathcal{C}$ with the set of torsion points is unlikely to be large unless the curve $\mathcal{C}$ is *special*.

Formally:

Let $H(X,Y) \in \mathbb{C}[X,Y]$ that has no nontrivial factor of the form $X^i - \rho Y^j$ or $X^i Y^j - \rho$ with a root of unity ρ. Then the equation $H(X,Y) = 0$ has only finitely many solutions (ζ_1, ζ_2) in which ζ_1, ζ_2 are roots of unity.

Beukers & Smyth (*2002*): bound for the number of torsion points on $\mathcal{C}$
Corvaja & Zannier (*2008*): bound for maximal order of torsion points on $\mathcal{C}$

Mult. dep. over $\overline{\mathbb{Q}}$: bounded height

Bombieri, Masser & Zannier (1999)

Assume $\varphi_1, \ldots, \varphi_m \in \mathbb{K}(X)$ are mult. indep. with constants. Then $\mathcal{S}$ is a set of bounded Weil height.

Remarks:

- $\mathcal{S}$ is an infinite set.
- The condition on $\varphi_1, \ldots, \varphi_m$ being mult. indep. with constants $\mathcal{C}$ is necessary, that is, it is not enough to be just mult. indep.

Example: Let $\varphi_1(X) = 2X$, $\varphi_2(X) = X^2$. Then h_1, h_2 are mult. indep., but there are infinitely many dependent values $(2^{m+1}, 2^{2m})$ for which the height is unbounded as $m \to \infty$.

Achieving finiteness: two mult. relations

Let

$$\mathcal{S}_1 = \Big\{\alpha \in \overline{\mathbb{Q}} : \prod_{i=1}^{m} \varphi_i(\alpha)^{k_i} = \prod_{i=1}^{m} \varphi_i(\alpha)^{\ell_i} = 1 \text{ for some lin. indep. } (k_1, \ldots, k_m), (\ell_1, \ldots, \ell_m) \in \mathbb{Z}^m \Big\}.$$

Bombieri, Masser & Zannier (1999)

Let $\varphi_1, \ldots, \varphi_m$ be as above. Then the set $\mathcal{S}_1$ is finite.

Bombieri, Masser & Zannier (*2003*): Extended the result above to rational functions defined over $\mathbb{C}$.

Maurin (*2008*): Weakened the assumption above to $\varphi_1, \ldots, \varphi_m$ not being mult. dep. only.

Going from $\overline{\mathbb{Q}}$ to proper subfields

Question: What further can one say on restricting the mult. dep. values defined over some $\mathbb{L} \subseteq \overline{\mathbb{Q}}$?

If $\mathbb{L}$ is a number field, then

Bombieri, Masser & Zannier (*1999*) + Northcott Theorem

$\Downarrow$

Finitely many dependent points $(\varphi_1(\alpha), \ldots, \varphi_m(\alpha))$**!**

Thus, it is only interesting to consider **infinite extensions** $\mathbb{K} \subseteq \mathbb{L} \subseteq \overline{\mathbb{Q}}$.

We obtain results for $\mathbb{L} = \mathbb{K}^{ab}$ the maximal abelian extension of $\mathbb{K}$ (and in particular, $\mathbb{Q}^c = \mathbb{Q}^{ab}$ and $\mathbb{K}^c \subseteq \mathbb{K}^{ab}$ if $\mathbb{K} \neq \mathbb{Q}$).

Mult. dep. over $\mathbb{K}^{ab}$

Bombieri, Masser & Zannier (*1999*): bounded height for

$$\mathcal{S}(\mathbb{K}^{ab}) = \mathcal{S} \cap \mathbb{K}^{ab} = \{\alpha \in \mathbb{K}^{ab} : \varphi_1(\alpha), \ldots, \varphi_m(\alpha) \text{ are mult. dep.}\}.$$

$|\overline{\alpha}|$: the house of $\alpha \in \overline{\mathbb{Q}}$ (i.e., the maximum of absolute values $|\sigma(\alpha)|$ of the conjugates $\sigma(\alpha)$ over $\mathbb{Q}$)

Question: Can we go even further and claim that $\mathcal{S}(\mathbb{K}^{ab})$ is a set of bounded house? ... NO!

Example: $\varphi_1(X) = X$, $\varphi_2(X) = X + 1$. For any root of unity ζ, let $\alpha = \frac{1}{\zeta - 1}$. Then, $\varphi_1(\alpha)$ and $\varphi_2(\alpha)$ are mult. dep., but $|\overline{\alpha}|$ grows with the order of ζ, and thus it's not bounded.

However this is essentially the only possible example!

O., Sha, Shparlinski & Zannier (2017)

Let $\varphi_1, \ldots, \varphi_m \in \mathbb{K}(X)$ *be monic and mult. indep. with constants. Then, there exists* $A \geq 1$*, depending only on* $[\mathbb{K} : \mathbb{Q}]$ *and* $\varphi_1, \ldots, \varphi_m$*, such that each element* $\alpha \in \mathcal{S}(\mathbb{K}^{ab})$ *satisfies* $[\mathbb{K}^c(\alpha) : \mathbb{K}^c] \leq A$ *and*

$$\alpha = \frac{\gamma}{1 - \eta},$$

where $\eta \in \mathbb{U}$*, and* $\gamma \in \mathbb{K}(\alpha)$ *with* $\overline{\gamma} \leq A$*.*

The proof is based on a combination of the following main tools:

- *Bombieri, Masser & Zannier* (*1999*): $\mathrm{h}(\alpha) \ll_{d,\varphi_1,\dots,\varphi_m} 1$, $d = [\mathbb{K} : \mathbb{Q}]$, for any $\alpha \in \mathcal{S}_{h_1,\dots,h_s}(\mathbb{K}^{ab})$;
- *Schlickewei* (*1997*): If we take Γ the finitely generated subgroup of $\overline{\mathbb{Q}}^*$ generated by $\varphi_1(\alpha), \dots, \varphi_m(\alpha)$ for some $\alpha \in \mathcal{S}(\mathbb{K}^{ab})$, then one can find 'good' generators $g_1, \dots, g_r \in \Gamma$ of a subgroup isomorphic to Γ/tors such that

$$\mathrm{h}(g_1^{a_1} \cdots g_r^{a_r}) \gg_r \sum_{i=1}^{r} |a_i| \mathrm{h}(g_i).$$

- *Amoroso & Zannier* (*2010*): Lehmer's conjecture holds: for any $\gamma \in \mathbb{K}^{ab} \setminus \mathbb{U}$, $h(\gamma) \gg_d 1$.

From all these, there exist $k_1, \dots, k_m \in \mathbb{Z}$, with

$$0 < \max |k_i| \ll_{d_{\mathbb{K}},\varphi_1,\dots,\varphi_m} 1,$$

and such that

$$\varphi_1(\alpha)^{k_1} \cdots \varphi_m(\alpha)^{k_m} \in \mathbb{U}.$$

If we invoke Cyclotomic Hilbert's Irreducibility Theorem, we obtain a **finiteness** result over $\mathbb{K}^{ab}$.

Dvornicich & Zannier (2007)

Let $f \in \mathbb{K}^c[X, Y]$ be such that $f(X, Y^m)$ as a polynomial in X does not have a root in $\mathbb{K}^c(Y)$ for all $m \leq \deg_X f$. Then, $f(X, \zeta)$ has a root in $\mathbb{K}^c$ for only finitely many $\zeta \in \mathbb{U}$.

We say that $\varphi_1, \ldots, \varphi_m \in \mathbb{K}(X)$ multiplicatively generate a power of a linear fractional transformation if there exists integers $c_1, \ldots, c_m$, not all zero, such that

$$\varphi_(X)^{c_1} \cdots \varphi_m(X)^{c_m} = \left(\frac{aX+b}{cX+d}\right)^m, \quad a, b, c, d \in \mathbb{K}, \quad m \geq 1.$$

Recall:

$$\mathcal{S}(\mathbb{K}^{ab}) = \mathcal{S} \cap \mathbb{K}^{ab} = \{\alpha \in \mathbb{K}^{ab} : \varphi_1(\alpha), \ldots, \varphi_m(\alpha) \text{ are mult. dep.}\}.$$

O., Sha, Shparlinski & Zannier (2017)

Assume that $\varphi_1, \ldots, \varphi_m$ are mult. indep. with constants and such that they cannot multiplicatively generate a power of a linear fractional transformation. Then, $\mathcal{S}(\mathbb{K}^{ab})$ is a finite set.

Linear dependence of points on elliptic curves

Notation & set-up

- K is a number field;
- E is an elliptic curve defined by a Weierstrass equation over $\mathbb{K}$:

$$Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{K}, \quad 4a^3 + 27b^2 \neq 0.$$

- O is the point at infinity of E;
- E_{tor} is the set of torsion points on $E(\overline{\mathbb{K}})$.

Linear dependence

The points $P_1, \ldots, P_n$ on E are linearly dependent (lin. dep.) if there exists a non-zero $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ such that

$$k_1 P_1 + \cdots + k_n P_n = O.$$

(The case $n = 1$ corresponds to P_1 being a torsion point.)

Otherwise they are called linearly independent (lin. indep.).

Some previous work

- *Mazur* (*1978*), *Merel* (*1995*): the order of torsion points on $E(\mathbb{K})$ is uniformly bounded.
- *Barroero & Sha* (*2020*): there are at most finitely many torsion points on $E(\overline{\mathbb{Q}})$ with multiplicatively dependent coordinates.

More generally one has:

Barroero & Sha (2020)

Let $f_1, \dots, f_n \in \mathbb{K}(X, Y)$ be mult. indep.. Then there are finitely many torsion points $(\alpha, \beta) \in E(\overline{\mathbb{Q}})$ such that $f_1(\alpha, \beta), \dots, f_n(\alpha, \beta)$ are mult. dep.

Remarks:

- If E has complex multiplication (CM), then $\mathbb{K}(E_{\mathrm{tor}}) \subset \mathbb{K}^{ab}$, and thus finiteness follows from *O., Sha, Shparlinski & Zannier* (*2019*).
- *Barroero & Sha* (*2020*): if $\mathbb{K}(E_{\mathrm{tor}})$ has the Bogomolov property, then the result above is effective. This is known for E with CM (*Amoroso & Zannier* (*2010*)) and for E defined over $\mathbb{Q}$ (*Habegger* (*2013*), *Frey* (*2018*)).

Several other works proving finiteness of points on curves in products of elliptic curves satisfying two independent relations:

Raynaud (*1983*), *Viada* (*2008*), *Galateau* (*2010*): two linear dependencies

Masser & Zannier (*2014*), *Bertrand, Masser, Pillay & Zannier* (*2016*), *Barroero & Capuano* (*2015, 2017*), . . . : considered families of elliptic curves in Legendre form, and looked at both linear and multiplicative dependencies

Let $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_m)$ and $\boldsymbol{\varrho} = (\varrho_1, \ldots, \varrho_n)$ be vectors of non-zero rational functions in $\mathbb{K}(X)$ and define

$$\mathcal{S}_2 = \{\alpha \in \overline{\mathbb{Q}} : \varphi_1(\alpha), \ldots, \varphi_m(\alpha) \text{ are mult. dep. and } (\varrho_1(\alpha), \cdot), \ldots, (\varrho_n(\alpha), \cdot) \text{ are lin. dep.}\}.$$

Following same strategy as in *Barroero & Capuano* (*2017*), one has:

Barroero, Capuano, Mérai, O. & Sha (2020)

Assume that $\varphi_1, \ldots, \varphi_m$ are mult. indep. and the points $(\varrho_1(X), \cdot), \ldots, (\varrho_n(X), \cdot)$ in $E(\overline{\mathbb{K}(X)})$ are lin. indep. over $\mathbb{Z}$. Suppose moreover that at least one of the following conditions holds:

1. *$\varphi_1, \ldots, \varphi_m$ are mult. indep. modulo constants;*
2. *the points $(\varrho_1(X), \cdot), \ldots, (\varrho_n(X), \cdot)$ are lin. indep. over $\mathrm{End}(E)$ modulo points in $E(\overline{\mathbb{Q}})$.*

Then the set $\mathcal{S}_2$ is finite.

If $n = 1$, *Barroero & Sha* (*2020*): $\#\mathcal{S}_2$ can be effectively bounded (over $\mathbb{Q}$)

Multiplicative and linear dependence for rational function values and points on elliptic curves in $\overline{\mathbb{F}}_p$

Goal

p is a prime, $\mathbb{F}_p$ the finite field with p elements

It is clear that the above finiteness results do not hold over $\overline{\mathbb{F}}_p$ since any element $\alpha \in \overline{\mathbb{F}}_p$ is a root of unity.

Main idea

We use the interplay between

$$\text{char} = 0 \quad \text{and} \quad \text{char} > 0,$$

i.e., we work with rational functions over $\mathbb{Z}$ and obtain results about the "size" of the sets multiplicatively and additively generated by values of rational functions and by points on an elliptic curve, respectively, in reduction modulo primes.

Some new notation

- $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_m), \boldsymbol{\varrho} = (\varrho_1, \ldots, \varrho_n) \in \mathbb{Q}(X)^n$ with non-zero components;
- E is an elliptic curve defined by a Weierstrass equation over $\mathbb{Q}$;
- E_p is the reduction of E modulo p;
- $\mathrm{ord}_p(\alpha)$ is the multiplicative order of $\alpha \in \overline{\mathbb{F}}_p^*$;
- $\mathrm{ord}_{E_p}(\alpha)$ is the order of the point (α, β) on the elliptic curve E_p for some $\beta \in \overline{\mathbb{F}}_p$ (if E_p is also an elliptic curve).

  Remark: $(\alpha, -\beta)$ has the same order as (α, β), so the definition of $\mathrm{ord}_{E_p}(\alpha)$ is kosher.

Previous work: order of points on algebraic varieties

Poonen's Conjecture – Informal

Unless there is a special geometric reason, the order of points $\mathbf{u}$ on an algebraic variety over $\overline{\mathbb{F}}_q$ is at least q^{dc} for some constant $c > 0$, where $d = [\mathbb{F}_q(\mathbf{u}) : \mathbb{F}_q]$.

There are several results giving lower bounds for the order of points of curves or higher dimensional varieties over $\overline{\mathbb{F}}_p$:

Voloch (*2007, 2010*), *Chang* (*2013*) (plane curves)

Chang, Kerr, Shparlinski and Zannier (*2014*) (algebraic varieties)

We generalise these results to multiplicative relations between values of rational fucntions.

Refinement of mult. dep. and lin. dep. in $\overline{\mathbb{F}}_p$

Definition (K-*multip. dep.*)

Let K be a positive integer. We say that elements $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{F}}_p^*$ are **K-mult. dep.** *if there exists a non-zero $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ such that*

$$\alpha_1^{k_1} \cdots \alpha_n^{k_n} = 1 \quad \textit{and} \quad \max_{i=1,\ldots,n} |k_i| \leq K.$$

Definition (L-*lin. dep.*)

Let L be a positive integer. We say that the points $P_1, \ldots, P_n$ on the reduction E_p of the elliptic curve E modulo p (assuming E_p is also an elliptic curve) are **L-lin. dep.** *if there exists a non-zero $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ such that*

$$k_1 P_1 + \cdots + k_n P_n = O \quad \textit{and} \quad \max_{i=1,\ldots,n} |k_i| \leq L.$$

Moreover, for any $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{F}}_p$, we say that the points

$$(\alpha_1, \cdot), \ldots, (\alpha_n, \cdot)$$

are *L-lin. dep.* if the points $(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n)$ are L-lin. dep. for some $\beta_1, \ldots, \beta_n \in \overline{\mathbb{F}}_p$ such that $(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n) \in E_p$.

Recall the sets:

$$\mathcal{S}_1 = \Big\{\alpha \in \overline{\mathbb{Q}} : \prod_{i=1}^{m} \varphi_i(\alpha)^{k_i} = \prod_{i=1}^{m} \varphi_i(\alpha)^{\ell_i} = 1 \text{ for some lin. indep. } (k_1, \ldots, k_m), (\ell_1, \ldots, \ell_m) \in \mathbb{Z}^m \Big\},$$

$$\mathcal{S}_2 = \big\{\alpha \in \overline{\mathbb{Q}} : \varphi_1(\alpha), \ldots, \varphi_m(\alpha) \text{ are mult. dep. and } (\varrho_1(\alpha), \cdot), \ldots, (\varrho_n(\alpha), \cdot) \text{ are lin. dep.}\big\},$$

which are **finite**.

Main objects of study

For positive integers $K, L \geq 1$ and prime p, we define the sets

$$\mathcal{A}_{\boldsymbol{\varphi},\boldsymbol{\varrho}}(p,K,L) = \{\alpha \in \overline{\mathbb{F}}_p : \prod_{i=1}^{m} \varphi_i(\alpha)^{k_i} = \prod_{i=1}^{m} \varphi_i(\alpha)^{\ell_i} = 1 \text{ for lin. indep.}$$

$$(k_1,\dots,k_m),(\ell_1,\dots,\ell_m) \in \mathbb{Z}^m,\ \max_{i=1,\dots,m} |k_i| \leq K,\ \max_{i=1,\dots,m} |\ell_i| \leq L\Big\},$$

$$\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p,K,L) = \Big\{\alpha \in \overline{\mathbb{F}}_p :\ \varphi_1(\alpha),\dots,\varphi_m(\alpha) \text{ are } K\text{-mult. dep.}$$
$$\text{and } (\varrho_1(\alpha),\cdot),\dots,(\varrho_n(\alpha),\cdot) \text{ are } L\text{-lin. dep.}\Big\}.$$

Goal: For sufficiently large primes p, prove that

$$\#\mathcal{A}_{\boldsymbol{\varphi},\boldsymbol{\varrho}}(p,K,L) \leq \#\mathcal{S}_1 \quad \text{and} \quad \mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p,K,L) \leq \#\mathcal{S}_2.$$

Remark: We omit here, but similar result holds for the set of $\alpha \in \overline{\mathbb{F}}_p$ such that $(\varrho_1(\alpha),\cdot),\dots,(\varrho_n(\alpha),\cdot)$ satisfy two independent K-lin. relations.

Two indep. mult. relations

Barroero, Capuano, Mérai, O. & Sha (2020)

Assume that $\varphi_1, \dots, \varphi_m$ are mult. indep. Then, there exists an effectively computable constant c_1 depending only on $\boldsymbol{\varphi}$ such that for arbitrary integers $K, L \geq 1$, and any prime $p > \exp(c_1 K L)$, we have

$$\#\mathcal{A}_{\boldsymbol{\varphi},\boldsymbol{\varrho}}(p, K, L) \leq \#\mathcal{S}_1,$$

where $\#\mathcal{S}_1$ is effectively computable, and the elements of $\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L)$ come from the reduction modulo p of elements of $\mathcal{S}_1$.

Kerr, Mello & Shparlinski (*2020*): obtained, for almost all primes p, a lower bound of the form $p^{1/(2m+2)+o(1)}$ for the order of all but finitely many vectors $(\varphi_1(\alpha), \dots, \varphi_m(\alpha))$, $\alpha \in \overline{\mathbb{F}}_p$, which satisfy two independent multiplicative relations.

There are three effectively computable constants c_1, c_2, c_3 depending only on φ_1, φ_2 such that (applying the above with $m = 2$, $K = L = \lceil c_3(\log p)^{1/2} \rceil$) for any prime $p > c_1$, for all but c_2 elements $\alpha \in \overline{\mathbb{F}}_p$ one has

$$\max\{\mathrm{ord}_p(\varphi_1(\alpha)), \mathrm{ord}_p(\varphi_2(\alpha))\} \geq c_3(\log p)^{1/2}.$$

This improves a result of *Chang* (*2013*):

$$\max\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\varphi(\alpha))\} \gg \left(\frac{\log p}{\log\log p}\right)^{1/2}.$$

Chang, Kerr, Shparlinski & Zannier (*2014*): improvement of same shape.

Mult. dep. & lin. dep.

Barroero, Capuano, Mérai, O. & Sha (2020)

Assume that $\varphi_1, \dots, \varphi_m$ *are mult. indep. and the points* $(\varrho_1(X), \cdot), \dots, (\varrho_n(X), \cdot)$ *in* $E(\overline{\mathbb{Q}(X)})$ *are lin. indep. over* $\mathbb{Z}$. *Suppose moreover that at least one of the following conditions holds:*

1. $\varphi_1, \dots, \varphi_m$ *are mult. indep. modulo constants;*
2. *the points* $(\varrho_1(X), \cdot), \dots, (\varrho_n(X), \cdot)$ *are lin. indep. over the* $\mathrm{End}(E)$ *modulo points in* $E(\overline{\mathbb{Q}})$.

Then, there exist an effectively computable constant c_1 *depending only on* $\boldsymbol{\varphi}, \boldsymbol{\varrho}, E$ *such that for any* $p > \exp(c_1 K L^2)$, *we have*

$$\#\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L) \leq \#\mathcal{S}_2,$$

and the elements of $\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L)$ *come from the reduction modulo* p *of elements of* $\mathcal{S}_2$.

There exist two effectively computable constants c_1, c_3 and a constant c_2 depending only on φ, ϱ, E such that (applying the above with $m = n = 1$, $K = L = \lceil c_3(\log p)^{1/3} \rceil$) for any prime $p > c_1$ and for all but c_2 elements $\alpha \in \overline{\mathbb{F}}_p$ we have

$$\max\{\mathrm{ord}_p(\varphi(\alpha)), \mathrm{ord}_{E_p}(\varrho(\alpha))\} \geq c_3(\log p)^{1/3}.$$

This extends *Voloch* (*2010*): for a point P on a fixed elliptic curve over $\mathbb{F}_q$, under some conditions, the order of the y-coordinate of P is large.

Barroero, Capuano, Mérai, O. & Sha (2020)

Under the conditions above, there exist an effectively computable constant c_1 and a constant c_2 both depending only on $\boldsymbol{\varphi}, \boldsymbol{\varrho}, E$ such that as $N \to \infty$, for all but $c_1 N(\log N)^{-2}$ primes $p \leq N$ and for all but at most c_2 elements $\alpha \in \overline{\mathbb{F}}_p$, either the order of the subgroup $\langle \varphi_1(\alpha), \ldots, \varphi_m(\alpha) \rangle$ in $\overline{\mathbb{F}}_p^*$ or the order of the subgroup $\langle (\varrho_1(\alpha), \cdot), \ldots, (\varrho_n(\alpha), \cdot) \rangle$ in $E(\overline{\mathbb{F}}_p)$ is at least

$$N^{mn/(2mn+m+n)}(\log N)^{-1/2}.$$

Moreover, when $n = 1$, the constant c_2 is also effectively computable.

Sketch of proof

- Capturing lin. dep. (*Semaev (2004)*): For $n \geq 2$, there exists $\sigma_n \in \mathbb{Z}[X_1, \ldots, X_n, a, b]$ (called the n-th summation polynomial) such that: for any $x_1, \ldots, x_n \in \overline{\mathbb{Q}}$, we have $\sigma_n(x_1, \ldots, x_n) = 0$ if and only if there are $y_1, \ldots, y_n \in \overline{\mathbb{Q}}$ such that $(x_i, y_i) \in E, 1 \leq i \leq n$, and

$$(x_1, y_1) + \cdots + (x_n, y_n) = O.$$

  Moreover, the polynomials σ_n can be defined recursively using resultants.
- Let ψ_n be the nth-division polynomial of E, $\phi_n = X\psi_n^2 - \psi_{n+1}\psi_{n-1}$, $n \geq 1$ and

$$\Psi_n = \begin{cases} \psi_n & \text{if } n \text{ is odd,} \\ \psi_n/Y & \text{if } n \text{ is even} \end{cases} \in \mathbb{Z}[a, b, X].$$

- (x, y) is an n-torsion point on E if $\Psi_n(x) = 0$ for $n \geq 3$ and 2-torsion if $y = 0$.
- If $P = (x, y)$ is not an n-torsion point, then the first coordinate of the point nP is $\frac{\phi_n(x)}{\psi_n^2(x)}$.

- Recall the sets

$$\mathcal{S}_2 = \big\{\alpha \in \overline{\mathbb{Q}} : \varphi_1(\alpha), \dots, \varphi_m(\alpha) \text{ are mult. dep.} \\ \text{and } (\varrho_1(\alpha), \cdot), \dots, (\varrho_n(\alpha), \cdot) \text{ are lin. dep.}\big\},$$

$$\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L) = \big\{\alpha \in \overline{\mathbb{F}}_p : \ \varphi_1(\alpha), \dots, \varphi_m(\alpha) \text{ are } K\text{-mult. dep.} \\ \text{and } (\varrho_1(\alpha), \cdot), \dots, (\varrho_n(\alpha), \cdot) \text{ are } L\text{-lin. dep.}\big\}.$$

- $\#\mathcal{S}_2 \ll_{\boldsymbol{\varphi},\boldsymbol{\varrho},E} 1$.
- For any $\boldsymbol{k} = (k_1, \dots, k_m) \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$ define

$$\Omega_{\boldsymbol{k}} = \varphi_1^{k_1} \dots \varphi_m^{k_m} \in \mathbb{Q}(X),$$

and $\boldsymbol{\ell} = (\ell_1, \dots, \ell_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ let $\Theta_{\boldsymbol{\ell}} \in \mathbb{Q}(X)$ be defined by

$$\Theta_{\boldsymbol{\ell}} = \begin{cases} \Psi_{\ell_1} \circ \varrho_1 & \text{if } n = 1, \\ \sigma_n \left(\frac{\phi_{\ell_1}}{\psi_{\ell_1}^2} \circ \varrho_1, \dots, \frac{\phi_{\ell_n}}{\psi_{\ell_n}^2} \circ \varrho_n \right) & \text{if } n \geq 2. \end{cases}$$

- Thus, $\mathcal{S}_2$ is the set of solutions $\alpha \in \overline{\mathbb{Q}}$ to the system of equations

$$\Omega_{\boldsymbol{k}}(X) - 1 = \Theta_{\boldsymbol{\ell}}(X) = 0 \quad \text{for some } \boldsymbol{k} \in \mathbb{Z}^m \setminus \{\mathbf{0}\} \text{ and } \boldsymbol{\ell} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}.$$

- Write

$$\Omega_{\boldsymbol{k}} = \frac{F_{\boldsymbol{k}}}{G_{\boldsymbol{k}}}, \quad \gcd(F_{\boldsymbol{k}}, G_{\boldsymbol{k}}) = 1, \quad \text{and} \quad \Theta_{\boldsymbol{\ell}} = \frac{U_{\boldsymbol{\ell}}}{V_{\boldsymbol{\ell}}}, \quad \gcd(U_{\boldsymbol{\ell}}, V_{\boldsymbol{\ell}}) = 1,$$

  with polynomials $F_{\boldsymbol{k}}, G_{\boldsymbol{k}}, U_{\boldsymbol{\ell}}, V_{\boldsymbol{\ell}} \in \mathbb{Z}[X]$.
- Then, the system of equations

$$F_{\boldsymbol{k}}(X) - G_{\boldsymbol{k}}(X) = \tilde{U}_{\boldsymbol{\ell}}(X) = 0$$

  has no solution over $\overline{\mathbb{Q}}$, where $\tilde{U}_{\boldsymbol{\ell}}$ is obtained from $U_{\boldsymbol{\ell}}$ by eliminating multiple factors and irreducible factors that have a root in the set $\mathcal{S}_2$.

$$\Downarrow$$

$$R_{\boldsymbol{k},\boldsymbol{\ell}} = \operatorname{Res}\left(F_{\boldsymbol{k}}(X) - G_{\boldsymbol{k}}(X), \tilde{U}_{\boldsymbol{\ell}}(X)\right) \text{ is non-zero.}$$

- If $p > |R_{\boldsymbol{k},\boldsymbol{\ell}}|$, then $p \nmid R_{\boldsymbol{k},\boldsymbol{\ell}}$, and therefore the system above has no solution over $\overline{\mathbb{F}}_p$. We can choose

$$p > \max_{\boldsymbol{k} \in \{0,\pm 1,\ldots,\pm K\}^m \setminus \{\mathbf{0}\}} \max_{\boldsymbol{\ell} \in \{0,\pm 1,\ldots,\pm L\}^n \setminus \{\mathbf{0}\}} |R_{\boldsymbol{k},\boldsymbol{\ell}}|.$$

- For $\boldsymbol{k} \in \{0, \pm 1, \dots, \pm K\}^m \setminus \{\mathbf{0}\}$ and $\boldsymbol{\ell} \in \{0, \pm 1, \dots, \pm L\}^n \setminus \{\mathbf{0}\}$, one has the bounds:

$$\deg(F_{\boldsymbol{k}} - G_{\boldsymbol{k}}) \ll_{\boldsymbol{\varphi}} K, \quad \mathrm{h}(F_{\boldsymbol{k}} - G_{\boldsymbol{k}}) \ll_{\boldsymbol{\varphi}} K,$$
$$\deg \tilde{U}_{\boldsymbol{\ell}} \ll_{\boldsymbol{\varrho}} L^2, \quad h(\tilde{U}_{\boldsymbol{\ell}}) \ll_{\boldsymbol{\varrho}, E} L^2.$$

$$\Downarrow$$

$$\log |R_{\boldsymbol{k},\boldsymbol{\ell}}| \ll_{\boldsymbol{\varphi},\boldsymbol{\varrho},E} KL^2.$$

- Therefore, when $p > \exp(c_1 KL^2)$, the system above has no solution over $\overline{\mathbb{F}}_p$ for any $\boldsymbol{k}, \boldsymbol{\ell}$ in the same ranges as above and we obtain

$$\#\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L) \leq \#\mathcal{S}_2.$$