

RESEARCH STATEMENT

RICARDO CONCEIÇÃO

1. INTRODUCTION

A seminal paper in Arithmetic Geometry is L.J. Mordell's [Mor22] "*On the rational solutions of the indeterminate equations of the third and fourth degrees*". In this paper we can find two statements that have greatly influenced not only number theory, but mathematics in general. First he proves that the group of rational points $E(\mathbb{Q})$ on any elliptic curve E is indeed finitely generated, a fact which was assumed by Poincaré. Since the group structure on $E(\mathbb{Q})$ is abelian, we can associate to it a natural number, the rank of $E(\mathbb{Q})$, which turns out to be in the center of many of the unresolved problems in Arithmetic Geometry and to have generated a great amount of work. One particular problem that has attracted much attention is the question of how large the rank of $E(\mathbb{Q})$ can be when we vary the elliptic curve E . Currently, it is conjectured that the rank can be arbitrarily large. We will refer to this as the *rank conjecture*.

The other statement contained in the aforementioned paper by Mordell is a question that remained unsolved for 61 years, whose solution was worthy of a Fields medal. The question, now known as Mordell's conjecture, was whether curves of genus ≥ 2 could have infinitely many rational points. Mordell believed that the answer to this question was 'no', and in 1983 G. Faltings proved he was right. After Falting's solution, the focus of research turned to the question of how such a statement could be generalized to varieties of higher dimension. Independently, Bombieri (only for surfaces) and Lang proposed a generalization to Mordell's conjecture that has survived the test of time. Here is what they expect:

Conjecture 1 (Lang-Bombieri). *If X is a variety of general type defined over a number field K , then the set $X(K)$ of K -rational points is not Zariski-dense.*

In our thesis [Con08] we dealt with the analogous statements of these two conjectures over the function field $\mathbb{F}_q(t)$ instead of \mathbb{Q} . The main result of [Con08] is the following

Theorem 2. *Suppose $q \equiv 3 \pmod{4}$ or $q \equiv 2 \pmod{3}$. Then there are quadratic and cubic twists of supersingular elliptic curves defined over $\mathbb{F}_q(t)$ containing arbitrarily many points with polynomial coordinates in different Frobenius orbits.*

Its proof follows from the following facts:

- Let $m \in \{3, 4\}$ and n be a fixed positive integer. For every odd divisor k of n , the congruence $q^k + 1 \equiv 0 \pmod{m}$ will allow us to construct a polynomial map from the curve defined by $D : v^m = u^{p^k} - u$ to a supersingular elliptic curve E ;

Date: December 18, 2008.

- The large group of automorphism of $C : s^2 = t^{q^n} - t$ will provide an “extra” polynomial map from C to D ;
- the composition of the two polynomial maps given above will yield an integral point on the quadratic ($m = 2$ case) or cubic ($m = 3$ case) twist of E by $t^{q^n} - t$.

Next we will discuss how this statement can be used to prove the rank conjecture and disprove a generalization of the Lang-Bombieri over $\mathbb{F}_q(t)$.

The rank conjecture over the function field $\mathbb{F}_q(t)$ has been proved by different people and in different situations, see [TS67], [Elk94], [Ulm02], [BDS04], [DS07], [Ulm07], [Ber08]. Their proofs boil down to the fact that, for an elliptic curve E defined over $\mathbb{F}_q(t)$, the rank of $E(\mathbb{F}_q(t))$ can be related to the order of vanishing of certain analytic functions: the ζ -function of a hyperelliptic curve, in the case of constant elliptic curves [TS67], [Elk94], [BDS04], [DS07]; and the L -function of E , in case E is non-constant [Ulm02], [Ulm07], [Ber08]. In any case, these proofs are rather indirect and cannot be used to find a large set of linearly independent points. The novelty of our approach lies in the fact that we construct isotrivial supersingular elliptic curves with high rank by explicitly providing an arbitrarily large set of points with polynomial coordinates that are later shown to be linearly independent.

In [CHM97], L. Caporaso, J. Harris and B. Mazur show how the Lang-Bombieri conjecture can be used to prove the following astounding result:

Theorem 3 (Uniformity Conjecture). *Suppose the Lang-Bombieri conjecture is true over a number field K . For any integer $g \geq 2$, there exists a positive constant B depending only on K and g , such that for every curve C/K of genus g , the number of K -rational points satisfy $|C(K)| \leq B$.*

As pointed by D. Abramovich [Abr97] one should expect that an analogous result holds, if rational points are replaced by integral points; and curves of genus $g \geq 2$ are replaced by elliptic curves. Indeed, by assuming the “quasi-projective” version of the Lang-Bombieri conjecture, the so called Lang-Vojta conjecture, he was able to provide a proof that over \mathbb{Q} the number of integral points on any semistable elliptic curve E can be bounded independently of E . As a very special case of the reasoning behind the proof of this statement, in [Con08] we are able to provide a simple proof to the following theorem contained in [Abr97]

Theorem 4. *Let $y^2 = x^3 + Ax + b$ be an elliptic curve where A and B are S -integers in a global field K . Suppose the Lang-Vojta conjecture is true over K . Then for any square-free S -integer t , the number of S -integral points in the quadratic twist $ty^2 = x^3 + Ax + B$ can be bounded independently of t .*

Since over $\mathbb{F}_q(t)$ points with polynomials coordinates are the analogous objects to integral points, what our *Theorem 2* shows is that some care should be taken if one wants to transport the Lang-Vojta conjecture to the function field case.

2. CURRENT AND FUTURE PROJECTS

In a talk given at the University of Texas at Austin in October 2008, D. Ulmer explained how one could use the approach provided by L. Berger [Ber08] to construct a family of non-constant elliptic curves over $\mathbb{F}_q(t)$ with arbitrarily large high rank and with an explicit set of linearly independent points generating a subgroup of

finite index. Inspired by this talk, we recently managed to show that the examples constructed in [Con08] can be seen in the general framework provided in [Ulm07]. Indeed, the curves $(t^{q^n} - t)y^2 = x^3 - x$ and $y^2 = x^3 + t^{q^n+1} + 1$ considered in our dissertation satisfy what Ulmer calls *Shioda's 4-monomial condition*, and we were able to use this interpretation to provide a more natural proof to *Lemma 2.3* in [Con08] – we show that the sections obtained in this lemma arise from “trivial” curves on some Fermat surface. We believe that this interpretation of our results can also be used to provide a hint on why one should not expect any polynomial points on $(t^{q^n} - t)y^2 = x^3 - x$, if $q \equiv 1 \pmod{4}$, or $(t^{q^n} - t)y^2 = x^3 + 1$, for q arbitrary. We also believe that under this new light, it will be possible to show that in the supersingular case the quadratic twist $(t^{q+1} + 1)y^2 = x^3 + 1$ has arbitrarily many points with coordinates whose denominators are divided by a fixed set of irreducible polynomials; in other words, this curve has a large number of S -integral points defined over $\mathbb{F}_q(t)$.

On a different front, we are trying to find a way to adapt the approach explained in [Ber08] to construct elliptic curves with many integral points.

One curious result that we managed to prove in [Con08] was

Theorem 5. *Let $E : y^2 = f(x)$ be an elliptic curve defined over \mathbb{F}_q . The quadratic twist $(t^{q^n} - t)y^2 = f(x)$ has an ∞ -integral point $(F(t), G(t))$ defined over \mathbb{F}_{q^n} satisfying $F' \neq 0$ and $2 \deg F \leq q^n - 1$ if and only if $q \equiv 3 \pmod{4}$ and E is isomorphic over \mathbb{F}_{q^n} to $ay^2 = x^3 - x$, for some $a \in \mathbb{F}_{q^n}$.*

The condition that the derivative F' is non-zero is an important one: there are infinitely many integral points not satisfying it – so it is indeed necessary if one expect an analogue of Siegel's theorem to hold in positive characteristic. Recently we realized that the condition on the degree of F is equivalent to saying that F is a minimal value set polynomial over \mathbb{F}_q , as described for instance in [CLMS61] and [Mil64]. In our dissertation, we construct many integral points on the curve $(t^{q^n} - t)y^2 = x^3 - x$, when $q \equiv 3 \pmod{4}$. Our proof of the above theorem is very similar to the work of Mills [Mil64] and we believe that we may use some of his ideas to prove that the points we have constructed are all the integral points on this curve.

One of the reasons that we are able to construct many integral points on the curve $(t^{q^n} - t)y^2 = x^3 - x$ is the fact that the hyperelliptic curve $s^2 = t^{q^n} - t$ has a large number of automorphism fixing the point at infinity. If $A(t)$ is an additive polynomial, then a similar fact is true for the curve C defined by $s^2 = A(t)$. If someone is able to construct a polynomial map from C to an elliptic curve E , we expect that a similar reasoning as the one carried in our dissertation may be used to produce elliptic curves with many integral points. Our hope is that the work of Garcia & Özbudak [GO07] on maximal plane curves defined by additive polynomials will provide us some insight on where to look for such maps: maximal curves are supersingular curves, and therefore they will have many morphisms to a supersingular elliptic curve. One thing that we already know is that if E is not isomorphic to $y^2 = x^3 - x$ and such a map exists, then its degree has to be greater than $(\deg A(t) - 1)/2$. As a future project, we intend to follow this direction to either construct other examples of elliptic curves with many integral points, or to prove that the existence of an integral point on the quadratic twist of an elliptic curve E by an additive polynomial imposes strong restrictions on the isomorphism class of E .

In a different direction, Herivelto Borges and I have recently been interested in finding good bounds for the number of rational points on curves over finite fields, in the case of a plane singular curve in the Frobenius non-classical class - a case where the results in the literature seems to be very scarce.

REFERENCES

- [Abr97] D. Abramovich, *Uniformity of stably integral points on elliptic curves*, *Inventiones Mathematicae* **127** (1997), 307–317.
- [BDS04] I. Bouw, C. Diem, and J. Scholten, *Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_q(t)$ with constant j -invariant*, *Manuscripta Mathematica* **114** (2004), 487–501.
- [Ber08] L. Berger, *Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields*, *Journal of Number Theory* **128** (2008), 3013–3030.
- [CHM97] L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points*, *Journal of the American Mathematical Society* **10** (1997), 1–36.
- [CLMS61] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus, *Polynomials over finite fields with minimal value sets*, *Mathematika*, Lond. **8** (1961), 121–130.
- [Con08] R. Conceição, *Twists of elliptic curves with many integral points over function fields*, Thesis (2008).
- [DS07] C. Diem and J. Scholten, *Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_q(t)$ with constant j -invariant II*, *Journal of Number Theory* **124** (2007), 31–41.
- [Elk94] N. D. Elkies, *Mordell-weil lattices in characteristic 2. I. construction and first properties*, *International Mathematics Research Notices* (1994), no. 8, 343 ff., approx. 18 pp. (electronic).
- [GO07] A. Garcia and F. Ozbudak, *Some maximal function fields and additive polynomials*, *Communications in Algebra* **35** (2007), 1553 – 1566.
- [Mil64] W. H. Mills, *Polynomials with minimal value sets*, *Pacific J. Math* **14** (1964), 225–241.
- [Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, *Proc. Cambridge Philos. Soc* **21** (1922), 179–192.
- [TS67] J. T. Tate and I. R. Safarevic, *The rank of elliptic curves*, *Dokl. Akad. Nauk SSSR* **175** (1967), 770–773.
- [Ulm02] D. Ulmer, *Elliptic curves with large rank over function fields*, *Annals of Mathematics* **155** (2002), 295–315.
- [Ulm07] ———, *L -functions with large analytic rank and abelian varieties with large algebraic rank over function fields*, *Inventiones Mathematicae* **167** (2007), 379–408.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS AT AUSTIN, AUSTIN, TX 78712-1082.
E-mail address: rconceic@math.utexas.edu