Rend. Lincei Mat. Appl. 19 (2008), 73–78

Number theory. — *On the maximal order of a torsion point on a curve in* $\mathbb{G}_\mathrm{m}^n$, by PIETRO CORVAJA and UMBERTO ZANNIER, communicated by U. Zannier on 8 February 2008.

ABSTRACT. — Let $\mathcal{C}$ be an irreducible algebraic curve in $\mathbb{G}_\mathrm{m}^2$; we are concerned with the maximal order $m = m(\mathcal{C})$ of a torsion point on $\mathcal{C}$. We suppose that $\mathcal{C}$ is defined over a number field k, that it is not a translate of an algebraic subgroup by a torsion point, and we denote by d its degree and by g its genus. It is known that $m \ll_{k,\epsilon} d^{2+\epsilon}$ for any $\epsilon > 0$, which, as shown below, is nearly best possible if only the degree is taken into account. Here, by means of a new method, we prove an upper bound (actually for curves in $\mathbb{G}_\mathrm{m}^n$) which implies in particular $m \ll_{k,\epsilon} (d\sqrt{d+g})^{1+\epsilon}$. This renders the above result and for small g it improves on it. The appearance of the genus seems to be a new feature in this kind of problem.

KEY WORDS: Torsion points on curves; cyclotomic equations; Diophantine equations.

MATHEMATICS SUBJECT CLASSIFICATION (2000): Primary 11G35; Secondary 11C08.

INTRODUCTION

A well-known old problem by Lang is to prove that *if a plane curve* $f(x, y) = 0$ *contains infinitely many points with roots of unity coordinates, then* f *has a 'special' factor, i.e. of the shape* $ax^m + by^m$ *or* $ax^m y^n + b$. Simple elegant solutions were given by Ihara, Serre, Tate and others [L]. We can rephrase the result by saying that *if a curve in the torus* $\mathbb{G}_\mathrm{m}^2$ [1] *contains infinitely many torsion points, then it contains a translate of some algebraic subgroup of* $\mathbb{G}_\mathrm{m}^2$ *of positive dimension*.

This result was generalized in several directions. Here we are concerned with a quantitative version, seeking *a bound for the maximal order of a torsion point on a curve in* $\mathbb{G}_\mathrm{m}^n$.

We remark that a different, though related, known problem is to estimate the *number of torsion points on the curve*. Concerning this last issue, we refer for instance to [BS]; in that paper it is proved in particular that *if* f *has no factor of the above-mentioned special shape, then the number of torsion points on the curve* $f(x, y) = 0$ *does not exceed* $22V(f)$ where $V(f)$ is the area of the Newton polygon of f. In particular, the bound is $\ll (\deg f)^2$.

Remarkably, these last bounds do not depend on the field of definition of f; on the contrary, such a dependence must clearly appear in a bound for the maximal order. We also note that the bounds for the number of torsion points imply a bound for the maximal order, as follows: Let $f(P) = 0$ for a torsion point P of exact order m, where f is defined over k and has no special factors. Then $f(P^\sigma) = 0$ for each conjugate P^σ of P over k. There are $\geq \phi(m)/[k : \mathbb{Q}]$ such conjugates and all of them are torsion, whence by the above

$$\phi(m) \ll [k : \mathbb{Q}](\deg f)^2. \tag{1}$$

See also Remark (v) for a quick deduction of a result only slightly weaker, given by (5).

[1] As usual, $\mathbb{G}_\mathrm{m}$ denotes the affine line deprived of the origin.

In Remark (iii) below we note that this estimate is sometimes essentially best possible and that in particular the exponent 2 attributed to $\deg f$ cannot be generally lowered. In this short note we prove, however, that for a given ground field k, (1) can actually be improved when the curve defined by f has small genus g. The appearance of the genus represents a new feature with respect to known estimates.

In the following, by the *degree* of a curve embedded in $\mathbb{G}_{\mathrm{m}}^n$ we mean as usual the maximum number of intersections with a hyperplane not containing the curve, and by its *genus* we mean the genus of a nonsingular projective model of it (we do not assume that the curve is nonsingular). By a *torsion point* in $\mathbb{G}_{\mathrm{m}}^n$ we mean a point whose coordinates are roots of unity, whereas by a *torsion coset* in $\mathbb{G}_{\mathrm{m}}^n$ we mean a translate of an algebraic subgroup by a torsion point. We have:

THEOREM 1. *Let $\mathcal{C}$ be an absolutely irreducible curve in $\mathbb{G}_{\mathrm{m}}^n$, of genus g and degree d, defined over a number field k, and let r be the minimal dimension of a torsion coset containing $\mathcal{C}$. Suppose that $r \geq 2$ and let $P \in \mathcal{C}(\overline{\mathbb{Q}})$ be a torsion point of order m. Then*

$$\phi(m)^3 m^{-2/r} \leq 108(r!)^{2/r}[k:\mathbb{Q}]^3 d^2(g-1+rd).$$

Specializing to the interesting case $n = r = 2$ we obtain:

COROLLARY. *Let $\mathcal{C}/k$ be an absolutely irreducible curve of genus g and degree d in $\mathbb{G}_{\mathrm{m}}^2$, not a torsion coset. Suppose that $P \in \mathcal{C}(\overline{\mathbb{Q}})$ is a torsion point of order m. Then*

$$\phi(m)^3 m^{-1} \leq 216[k:\mathbb{Q}]^3 d^2(g-1+2d).$$

REMARKS. (i) Recall that $\phi(m) \gg m/\log\log m$, so the inequality in Theorem 1 yields

$$m(\log\log m)^{-\frac{3r}{3r-2}} \ll r[k:\mathbb{Q}]^{\frac{3r}{3r-2}} d^{\frac{2r}{3r-2}} (d+g)^{\frac{r}{3r-2}}$$

with a computable absolute implied constant, and for the Corollary

$$m(\log\log m)^{-3/2} \ll [k:\mathbb{Q}]^{3/2} d\sqrt{d+g}.$$

In this last case of a curve in $\mathbb{G}_{\mathrm{m}}^2$, the upper bound $g \leq (d-1)(d-2)/2$ gives in particular $m \ll_{k,\epsilon} d^{2+\epsilon}$ for every $\epsilon > 0$, which is near to (1). But when for instance k is fixed and g is much smaller than the above upper bound we actually improve on (1). (E.g., the bound $g \ll d^{\delta}$ for fixed $\delta < 2$ replaces the exponent 2 for $d = \deg f$ in (1) by $1+\frac{1}{2}\max(1,\delta)+\epsilon$.)

(ii) For $g = 0$ (actually $g \ll d$ suffices) and for instance $k = \mathbb{Q}$ we obtain in the Corollary a bound $m \ll_{\epsilon} d^{3/2+\epsilon}$ for the maximal order m. This yields the following statement: *let $R(t), S(t) \in \mathbb{Q}(t)$ be multiplicatively independent rational functions of degree $\leq d$ and suppose that for an algebraic number t_0 both $R(t_0), S(t_0)$ are roots of unity of common order m. Then $m \ll_{\epsilon} d^{3/2+\epsilon}$.* [2] Can this estimate be improved? The choice $R(t) = t$, $S(t) = 1+t+\cdots+t^{l-2}$ says that infinitely often we have $m \geq 2(d+2)$. So, for rational curves we may locate the 'correct' exponent for d in the interval $[1, 3/2]$. How to gain a sharper information? We do not know.

[2] This case of rational functions is relevant in [AR].

(iii) As anticipated, we prove that (1) is sometimes essentially best possible, so we cannot expect improvements if we do not take into account invariants other than the degree. Let p be a prime number, ζ be a primitive p-th root of 1 and set $R := [\sqrt{p}] + 1$. For each integer n with $0 \leq n \leq p-1$, we can divide n by R, obtaining $n = qR + r$, $q = q_n$, $r = r_n$, with $0 \leq r < R$. Form the polynomial $f(x, y) = \sum_{n=0}^{p-1} x^q y^r$, which has degree $d \leq ((p-1)/R) + R - 1 < 2\sqrt{p}$ and satisfies $f(\zeta^R, \zeta) = 0$. We prove that f is absolutely irreducible, so in particular it has no special factors, i.e. it defines an irreducible curve $\mathcal{C}$ which is not a coset of an algebraic subgroup. Letting $p - 1 = QR + s$ with $0 \leq s < R$, we observe that $s + 1$ is coprime to R, for their gcd divides the prime p. We have

$$f(x, y) = A(y)(1 + x + \cdots + x^{Q-1}) + B(y)x^Q,$$

where $A(y) = 1 + y + \cdots + y^{R-1}$, $B(y) = 1 + \cdots + y^s$. Since $s + 1$ is coprime to R, $A(y)$ and $B(y)$ are coprime polynomials. Also, $A(y)$ has no multiple roots. Then, by applying Eisenstein's criterion to the coefficient ring $\overline{\mathbb{Q}}[y]$ and the prime $y - \rho$ where ρ is a root of $A(y)$, the claim follows.

The maximal order of a torsion point on the curve $\mathcal{C}$ is now $\geq p \geq (\deg f)^2/4$, proving in particular (for $k = \mathbb{Q}$) that the exponent 2 of $\deg f$ in (1) cannot be generally lowered.

(iv) For fixed k, our bound involves both genus and degree, whereas (1) involves only the degree. On the other hand, the order of a torsion point cannot be estimated in terms of the genus only. In fact, for a prime $p > 2$ consider the plane curve $\mathcal{C} = \mathcal{C}_p$ of genus zero defined by $y = 1 + x + \cdots + x^{p-2}$. Plainly, $\mathcal{C}$ is irreducible, not a torsion coset and contains the point $(e^{2\pi i/p}, -e^{-2\pi i/p})$ of order $2p$.

A somewhat striking feature of our method is that its main new point is a kind of zero estimate over function fields (see Thm. CZ below) rather than some arithmetical tool. This has been carried out in the recent paper [CZ1] and is a function-field sharp analogue of a previous arithmetical result proved in [CZ2].

PROOF OF THEOREM 1. We let $\tilde{\mathcal{C}}$ be a complete nonsingular curve birational to $\mathcal{C}$, so in particular we have a birational surjective regular map $\pi : \tilde{\mathcal{C}} \to \overline{\mathcal{C}}$, where $\overline{\mathcal{C}}$ is the closure of $\mathcal{C}$ in $\mathbb{P}_n$. We shall need the following result, proved in [CZ1] (see Cor. 2.3(i) therein). We let S be a finite subset of $\tilde{\mathcal{C}}(\overline{\mathbb{Q}})$ and $\mathcal{O}_S^*$ be the group of rational functions in $\overline{\mathbb{Q}}(\mathcal{C})$ with all zeros and poles in S. For a rational function $u \in \overline{\mathbb{Q}}(\tilde{\mathcal{C}})^* = \overline{\mathbb{Q}}(\mathcal{C})^*$ we denote by $h(u)$ its degree (i.e. the number of poles of u in $\tilde{\mathcal{C}}$), stipulating that it is 0 if u is constant.

THEOREM CZ ([CZ1, Cor. 2.3(i)]). *Let $u, v \in \mathcal{O}_S^*$ be multiplicatively independent and not both constant. Then, setting $\chi := 2g - 2 + \#S$, we have*

$$\sum_{P \in \tilde{\mathcal{C}} \setminus S} \min\{\mathrm{ord}_P(1-u), \mathrm{ord}_P(1-v)\} \leq 3\sqrt[3]{2} \cdot (h(u)h(v)\chi)^{1/3}.$$

We proceed to the proof of Theorem 1, recalling the notation $d := \deg \mathcal{C}$. Renumbering coordinates, we may assume that $x_1, \ldots, x_r$ are multiplicatively independent as functions on $\mathcal{C}$, so they generate in $\bar{k}(\mathcal{C})^*$ a multiplicative subgroup isomorphic to $\mathbb{Z}^r$. As is customary, we may then define a norm on $\mathbb{Z}^r$ by setting $\|(a_1, \ldots, a_r)\| := h(x_1^{a_1} \cdots x_r^{a_r})$.

This can be extended first to $\mathbb{Q}^r$ by $h(x^l) := |l|h(x)$ and then to a nonnegative function on $\mathbb{R}^r$ by continuity. (See e.g. [BG, p. 136]; here we do not need the known fact that the extension is a norm.)

We let R be the region in $\mathbb{R}^r$ defined by $\|\mathbf{a}\| \leq 1$; it is clearly a closed convex region, symmetrical around the origin and has a volume, denoted $\mathrm{vol}(R)$. Observe that a given coordinate function x_i assumes a given value at most d times on $\mathcal{C}$, hence $h(x_i) \leq d$; in turn this implies $\|(a_1, \dots, a_r)\| \leq (\sum |a_i|)d$. In particular, R contains the region defined by $\sum |a_i| \leq d^{-1}$ and hence

$$\mathrm{vol}(R) \geq \frac{2^r}{r!} d^{-r}. \tag{2}$$

Let now $P = (\zeta_1, \dots, \zeta_n)$ be a torsion point on $\mathcal{C}$, of exact order m, and let Λ be the lattice in $\mathbb{Z}^r$ consisting of integer vectors $(l_1, \dots, l_r)$ with $\zeta_1^{l_1} \cdots \zeta_r^{l_r} = 1$. Since the map $(l_1, \dots, l_r) \mapsto \zeta_1^{l_1} \cdots \zeta_r^{l_r}$ is a homomorphism taking values in a group of order m, we deduce that $\mathrm{vol}(\Lambda)$ is a divisor of m.

Now, let $\lambda_1, \dots, \lambda_r$ be the successive minima with respect to R and Λ; they are defined by the fact that λ_i is the minimal real number such that $\lambda_i R$ contains i linearly independent points of Λ. By Minkowski's Second Theorem they satisfy $\lambda_1 \cdots \lambda_r \mathrm{vol}(R) \leq 2^r \mathrm{vol}(\Lambda) \leq 2^r m$ so in particular, taking also (2) into account,

$$\lambda_1 \lambda_2 \leq (2^r m/\mathrm{vol}(R))^{2/r} \leq (r!m)^{2/r} d^2. \tag{3}$$

Let $\mathbf{a} = (a_1, \dots, a_r)$ be a nonzero integer point in $\Lambda \cap \lambda_1 R$ and let $\mathbf{b} = (b_1, \dots, b_r)$ be an integer point in $\Lambda \cap \lambda_2 R$, linearly independent of $\mathbf{a}$. We set $u := x_1^{a_1} \cdots x_r^{a_r}$, $v := x_1^{b_1} \cdots x_r^{b_r}$, so u, v are rational functions on $\mathcal{C}$. Then we have

$$h(u) \leq \lambda_1, \qquad h(v) \leq \lambda_2. \tag{4}$$

Also, u, v are multiplicatively independent, because $x_1, \dots, x_r$ are multiplicatively independent on $\mathcal{C}$ and $\mathbf{a}, \mathbf{b}$ are linearly independent; this also implies that none can be constant, because $u(P) = v(P) = 1$, as follows from the very definition of Λ.

(For $r = n = 2$ we could now apply Bézout's theorem to an equation $f(x_1, x_2) = 0$ for the curve, together with $u(x_1, x_2) = 1$ to obtain a bound for the number of conjugates of P. See Remark (v) for this 'intersection' method, which is also at the basis of the paper [BS].)

Since $u(P) = v(P) = 1$ and since $\mathcal{C}$ is defined over k we also have $u(P^\sigma) = v(P^\sigma) = 1$ for all conjugates P^σ of P over k. There are at least $\phi(m)/[k : \mathbb{Q}]$ distinct such conjugates.

Naturally, u, v induce functions $\tilde{u} = u \circ \pi$, $\tilde{v} = v \circ \pi$ on $\tilde{\mathcal{C}}$. We apply Theorem CZ to them, by defining $S \subset \tilde{\mathcal{C}}$ as the union of the sets of zeros and poles of $\tilde{u}, \tilde{v}$. Every point $P^\sigma \in \mathcal{C}$ lifts to at least one point $Q_\sigma \in \tilde{\mathcal{C}}$, that is, $\pi(Q_\sigma) = P^\sigma$; of course distinct P^σ yield distinct Q_σ so the number of Q_σ is at least $\phi(m)/[k : \mathbb{Q}]$. Also, we have $\tilde{u}(Q_\sigma) = u(P^\sigma) = 1$ and similarly $\tilde{v}(Q_\sigma) = 1$. Hence Theorem CZ applied to $\tilde{u}, \tilde{v}$ yields

$$\phi(m) \leq [k : \mathbb{Q}] 3\sqrt[3]{2} (h(u)h(v)\chi)^{1/3},$$

whence, by (3) and (4),

$$\phi(m) \le [k:\mathbb{Q}]3\sqrt[3]{2}((r!m)^{2/r}d^2\chi)^{1/3}.$$

Recall that each coordinate has degree $\le d$, so has at most d zeros and at most d poles. Hence $\#S \le 2rd$, whence $\chi = 2g-2+\#S \le 2g-2+2rd$ and

$$\phi(m) \le [k:\mathbb{Q}]3\sqrt[3]{2}((r!m)^{2/r}d^2(2g-2+2rd))^{1/3}.$$

Cubing both sides we obtain the sought result, concluding the proof.

A METHODOLOGICAL POINT. Note that in the course of this proof we have worked in $\mathbb{G}_{\mathrm{m}}^r$ rather than $\mathbb{G}_{\mathrm{m}}^n$, considering only the first r coordinates; at first sight one could expect difficulties if $r < n$, since the order of a torsion point might decrease under projection to a proper subset of coordinates. In fact, this obstacle would actually appear if we tried to derive the proof by projection, after separate treatment of the case $r = n$. Instead, in the above approach we recover the possible loss through Theorem CZ, which takes into account all the points in a nonsingular model, not merely the geometric points in an embedding.

FURTHER REMARKS

(v) With a notation similar to this proof, working in $\mathbb{G}_{\mathrm{m}}^2$, let now R be the region in $\mathbb{R}^2$ defined by $|x|+|y| \le 1$ and let ξ_1 be the first minimum relative to it and the same lattice Λ, with corresponding integer vector (a,b). Observe that the torsion point P and its conjugates over k lie in the intersection of $\mathcal{C}$ with the curve defined by $X^aY^b = 1$. Hence by the Bézout theorem the number of conjugates is $\le d\xi_1 \le d\sqrt{2m}$. This leads to

$$\phi(m)^2m^{-1} \ll [k:\mathbb{Q}]^2d^2, \tag{5}$$

which in turn yields, for fixed k, a bound for m only slightly weaker than (1).

(vi) In the proof we have used the lower bound (2) for $\mathrm{vol}(R)$, derived from $h(x_i) \le d$. In special cases R may have a larger volume, improving the estimates. Also, one can replace the factor $g-1+rd$ by $g-1+(\#S/2)$, where S is the total number of zeros/poles of the x_i. Again, in special cases $\#S$ may be smaller than $2rd$, leading to a sharpening.

ACKNOWLEDGMENTS. It is a pleasure to thank Zeev Rudnick for helpful comments.

REFERENCES

[AR] N. AILON - Z. RUDNICK, *Torsion points on curves and common divisors of a^k-1 and b^k-1*. Acta Arith. 113 (2004), 31–38.

[BS] F. BEUKERS - C. SMYTH, *Cyclotomic points on curves*. In: Number Theory for the Millennium, 1 (Urbana, IL, 2000), A K Peters, 2002, 67–85.

[BG] E. BOMBIERI - W. GUBLER, *Heights in Diophantine Geometry*. Cambridge Univ. Press, 2006.

[CZ1] P. CORVAJA - U. ZANNIER, *Some cases of Vojta's conjecture on integral points over function fields*. J. Algebraic Geom. 17 (2008), 275–294.

[CZ2] P. CORVAJA - U. ZANNIER, *A lower bound for the height of a rational function at s-unit points*. Monatsh. Math. 144 (2005), 203–224.

[L] S. LANG, *Fundamentals of Diophantine Geometry*. Springer, 1983.

Received 27 March 2007,
and in revised form 8 May 2007.

P. Corvaja
Dipartimento di Matematica
Università di Udine
Via Delle Scienze
33100 UDINE, Italy
corvaja@dimi.uniud.it

U. Zannier
Scuola Normale Superiore
Piazza dei Cavalieri 7
56126 PISA, Italy
u.zannier@sns.it