BULLETIN DE LA S. M. F.

J.F. VOLOCH

A Diophantine problem on algebraic curves over function fields of positive characteristic

Bulletin de la S. M. F., tome 119, nº 1 (1991), p. 121-126
<http://www.numdam.org/item?id=BSMF_1991__119_1_121_0>

Bull. Soc. math. France,
119, 1991, p. 121–126.

A DIOPHANTINE PROBLEM ON ALGEBRAIC CURVES OVER FUNCTION FIELDS OF POSITIVE CHARACTERISTIC

BY

J.F. VOLOCH (*)

RÉSUMÉ. — Soit K un corps de fonctions d'une variable sur un corps fini de caractéristique p. On détermine les courbes algébriques sur K ayant une fonction K-rationnelle dont leurs valeurs dans une infinité de points K-rationnels sont des puissances p-èmes. On en déduit la finitude de l'ensemble des points rationnels des courbes sur K qui changent de genre sous une extension de corps de base.

ABSTRACT. — Let K be a function field in one variable over a finite field of characteristic p. We determine the algebraic curves over K having a K-rational function on it whose value at infinitely many K-rational points is a p-th power. From this we deduce the finiteness of the set of K-rational points of curves over K that change genus under ground-field extension.

1. Introduction

Let K be a function field in one variable over a finite field of characteristic p. The purpose of this paper is to characterize the algebraic curves X/K and the rational functions $f \in K(X)$ such that $f(P) \in K^p$ for infinitely many rational points $P \in X(K)$. This problem ties up with a question left open by SAMUEL [2] in his extension to positive characteristic of GRAUERT's proof of MORDELL's conjecture for function fields of characteristic zero. The question occurs when the relative genus of X/K is different from the absolute genus of X in the sense of [2] (or equivalently when $K(X)$ is a non-conservative function field in the sense of [1]).

The genus of a curve X defined over K, relative to K, can be defined as follows. It is the integer g for which $\ell(D) = \deg D + 1 - g$, for divisors D, defined over K, with degree $\deg D$ sufficiently large, where $\ell(D)$ is the dimension, as a K-vector space, of the space of rational functions on X,

(*) Texte reçu le 4 mai 1990, révisé le 13 septembre 1990.
J.F. VOLOCH, I.M.P.A., Estrada Dona Castorina 110, Rio de Janeiro 22460, Brésil.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037–9484/1991/121/$ 5.00

defined over K, with polar divisor bounded by D. The above definition of the genus depends on K. The genus of X, relative to K, does not change under separable extensions of K but may decrease under inseparable extensions. The absolute genus of X is thus defined as the genus of X relative to the algebraic closure of K. A standard example, for $p \geq 3$, is the curve $y^2 = x^p - a$. If $a \in K \backslash K^p$, then its genus, relative to K, is $\frac{1}{2}(p-1)$ and its absolute genus is 0.

SAMUEL showed that, with notation as above, $X(K)$ is finite if the absolute genus of X is at least two [2, Chapitre III, Theorem 1 and app. 2] and therefore the problem above is trivial for those curves. The question left open by SAMUEL [2, page 3] is whether curves with relative genus at least two and absolute genus 0 or 1 have finitely many rational points and we solve this question in the affirmative. Note that we have shown previously [4] that curves with relative genus 1 and absolute genus 0 have finitely many rational points (this will also follow from THEOREM 1 below). Hence all curves that admit genus change have finitely many rational points.

The paper is organized as follows. In sections 2 and 3 we solve our basic problem for rational curves and elliptic curves, respectively, and in section 4 we use these results to show that curves that admit genus change have finitely many rational points. Finally, we obtain the general solution to our problem.

2. Rational curves

Recall that K is a function field in one variable over a finite field of characteristic p. Let $t \in K \setminus K^p$ and $\delta = \mathrm{d}/\mathrm{d}t$, a derivation of K. If x is a variable over K, we extend δ to $K(x)$ by $\delta(x) = 0$. We shall also use the notation $r^{\delta}(x)$ for the action of δ on $r(x) \in K(x)$.

THEOREM 1. — *Let $r(x) \in K(x)$ be a rational function such that the set $\{a \in K \mid r(a) \in K^p\}$ is infinite. Then, there exists $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(K)$ such that $r((\alpha x + \beta)/(\gamma x + \delta)) \in K^p(x)$.*

Proof. — Multiplying, if necessary, $r(x)$ by the p-th power of its denominator, we can assume that $r(x)$ is a polynomial. Let n be the degree of $r(x)$ and assume first that $p \nmid n$.

Let $r(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$. By changing, if necessary, the variable x to $a_0^m x$, where $mn + 1 \equiv 0 \ (p)$, we can assume that $a_0 \in K^p$. Further, dividing $r(x)$ by a_0, we can also assume that $a_0 = 1$. Finally, changing x to $x - a_1/n$, we can assume that $a_1 = 0$.

If $a \in K$ is such that $r(a) \in K^p$, then

$$0 = \delta(r(a)) = r'(a)\delta a + r^\delta(a). \tag{*}$$

Note that $r^\delta(a) = \delta a_2 x^{n-2} + \cdots + \delta a_n$ is of degree at most $(n-2)$. If $r^\delta(x)$ is identically zero, then $r(x) \in K^p[x]$, as desired. Assume then that $r^\delta(x) \neq 0$.

Let v be a place of K with $v(a_i) \geq 0$, $i = 0, \ldots, n$ and $v(\mathrm{d}t) = 0$. If $a \in K$ is such that $v(a) < 0$ then, clearly, $v(r^\delta(a)) \geq (n-2)v(a)$ and $v(r'(a)) = (n-1)v(a)$, whence $v(\delta a) \geq 0$, from (*). If $v(a) \geq 0$ then, obviously, $v(\delta a) \geq 0$, as well. Thus $v(\delta a) \geq 0$ for all but finitely many places of K.

Further, the rational function $-r^\delta(x)/r'(x)$ has a zero at infinity. Thus, for any place v of K, if a has a sufficiently large pole at 0 then $\delta a = -r^\delta(a)/r'(a)$ satisfies $v(\delta a) \geq 0$, say. On the other hand, if $v(a)$ is bounded below, then $v(\delta a)$ is also bounded below. The conclusion of the above discussion is that there exists a divisor D of K such that $\delta a \in L(D)$ for any $a \in K$ with $r(a) \in K^p$. Hence, δa can assume finitely many values $b_1, \ldots, b_N$ for those a. The polynomial equations $r'(x)b_i + r^\delta(x) = 0$, $i = 1, \ldots, N$, have finitely many solutions unless one of them is identically zero. In the latter case, looking at the coefficient in x^{n-1}, it follows that $b_i = 0$ (recall that $p \nmid n$) and so $r^\delta(x) = 0$, contrary to the hypothesis. This proves the result when $p \nmid n$.

Let now $r(x)$ be a polynomial of degree $n \equiv 0$ (p) satisfying the hypothesis of the theorem. Let $a \in K$ be such that $r(a) \in K^p$. To prove the theorem for $r(x)$ it suffices to prove the theorem for the polynomial $x^n(r(1/x + a) - r(a))$, which has degree strictly less than n. The theorem now follows by induction on n.

Remark 1. — Let $r(x) \in K(x)$ be such that there exists $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(K)$ with $r((\alpha x + \beta)/(\gamma x + \delta)) \in K^p(x)$. Then $r(a) \in K^p$ for infinitely many $a \in K$. Indeed $r((\alpha x^p + \beta)/(\gamma x^p + \delta)) = (s(x))^p$ for some $s(x) \in K(x)$. This also shows that the curve $y^p = r(x)$ is parametrizable over K, that is, has relative genus zero over K.

Remark 2. — Theorem 1 contains, as special cases, the results of [4]. The proof of Theorem 1 is an extension of the techniques of [4].

3. Elliptic curves

We keep the notation of section 2. In particular, recall the derivation δ of K. If E/K is an elliptic curve given by the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, let $E^{(p)}/K$ be the elliptic curve with Weierstrass equation $y^2 + a_1^pxy + a_3^py = x^3 + a_2^px^2 + a_4^px + a_6^p$ and $F : E \to E^{(p)}$ be the Frobenius map defined by $F(x,y) = (x^p, y^p)$. Let also $V : E^{(p)} \to E$ be the isogeny dual to F. We extend δ to a derivation on $K(E^{(p)}) = K(x,y)$ by $\delta(x) = \delta(y) = 0$. As in section 2 we also denote by r^δ the action of δ on $r \in K(E^{(p)})$.

THEOREM 2. — *Notation as above. If $r \in K(E^{(p)})$ is such that the set $\{P \in E^{(p)}(K) \mid r(P) \in K^p\}$ is infinite, then there exists $P_0 \in E^{(p)}(K)$ such that the function $P \mapsto r(P + P_0)$ belongs to $K^p(E^{(p)})$. If $r \in K(E)$ is such that the set $\{P \in E(K) \mid r(P) \in K^p\}$ is infinite, then there exists $P_0 \in E(K)$ such that the function $P \mapsto r(V(P)+P_0)$ belongs to $K^p(E^{(p)})$.*

Proof. — Let $r \in K(E^{(p)})$ satisfy the hypothesis of the theorem. As $E^{(p)}(K)/F(E(K))$ is finite (by the Mordell-Weil theorem) it follows that there exists $P_0 \in E^{(p)}(K)$ such that, for infinitely many $P \in F(E(K))$, $r(P + P_0) \in K^p$. Let $s \in K(E^{(p)})$ be defined by $s(P) = r(P + P_0)$. If $P \in F(E(K))$, its x, y coordinates are p-th powers, hence $\delta(s(P)) = s^\delta(P)$. If, furthermore, $s(P) \in K^p$ then $s^\delta(P) = 0$. But s^δ has finitely many zeros unless is identically zero. We therefore conclude that $s^\delta = 0$, that is, $s \in K^p(E^{(p)})$, as desired.

Let $r \in K(E)$ satisfy the hypothesis of the theorem. Again by Mordell-Weil, $E(K)/V(E^{(p)}(K))$ is finite : there exists $P_1 \in E(K)$ such that there exists infinitely many $P \in V(E^{(p)}(K))$ with $r(P + P_1) \in K^p$. Thus, the function $P \mapsto r(V(P)+P_1)$ on $E^{(p)}$, satisfies the hypothesis of the theorem and, by what was proved above, there exists P_2 such that the function $P \mapsto r(V(P + P_2) + P_1)$ belongs to $K^p(E^{(p)})$ and the theorem follows with $P_0 = P_1 + V(P_2)$.

REMARK 3. — If $r \in K(E^{(p)})$ is such that $P \mapsto r(P + P_0)$ belongs to $K^p(E^{(p)})$ for some $P_0 \in E^{(p)}(K)$ then $r(P) \in K^p$ for all $P \in E^{(p)}(K)$, $P - P_0 \in F(E(K))$. Indeed $r(F(P) + P_0) = (s(P))^p$ for some $s \in K(E)$. Thus the cover of $E^{(p)}$ defined by the equation $z^p = r$ has genus 1 over K, since it is covered by E by the map $P \mapsto (F(P) + P_0, s(P))$. A similar phenomenon occurs for $r \in K(E)$ such that $P \mapsto r(V(P) + P_0)$ belongs to $K^p(E^{(p)})$. Indeed, $r(pP + P_0) = s(P)^p$ for some $s \in K(E)$, since $V \circ F$ is multiplication by p on E.