BULL. AUSTRAL. MATH. SOC. 11R58, 14G25
VOL. 41 (1990) [149–150]

MORDELL'S EQUATION IN CHARACTERISTIC THREE

J.F. VOLOCH

Let K be a function field in one variable over a finite field of characteristic three. If $a \in K$ is not a cube, we show that the equation $y^2 = x^3 + a$ has only finitely many solutions $x, y \in K$.

In this note we will study the equation $y^2 = x^3 + a, \quad a \in K$, where K is a function field in one variable over the perfect field k, of characteristic 3.

The analogous equation over $\mathbf{Q}$ is called Mordell's equation and has been extensively studied by Mordell and others ([**2**]). Over a field of characteristic not equal to 2 or 3, the equation $y^2 = x^3 + a, \quad a \neq 0$ defines an elliptic curve. In these cases the general theory of elliptic curves can be brought to bear on the problem ([**4**]).

In characteristic 3, the equation $y^2 = x^3 + a$ defines a rational curve over $\overline{K}$ but, if a is not a cube, it is a curve of genus 1 over K (under the definition of genus of [**1**], for example). When $a = b^3$ then the change of variables $x = x_1 - b$ takes the equation to $y^2 = x_1^3$ which has as general solution $x_1 = t^2, \quad y = t^3, \quad t \in K$. When $a \notin K^3$ the result is surprisingly different. The following result is a corollary of the theorem below.

COROLLARY. *If k is a finite field and $a \in K \setminus K^3$ then $y^2 = x^3 + a$ has only finitely many solutions $x, y \in K$.*

Before stating our theorem let is introduce some notation. Let C be the curve $y^2 = x^3 + a, \quad a \in K \setminus K^3$ and denote by $C(L)$ the L- rational points of C for $L \supset K$, any field. Since C is a cubic we can define a group law on the nonsingular (projective) points of $C(\overline{K})$ by the usual chord and tangent method. The singular point of C is $(-a^{1/3}, 0)$ which is not on $C(K)$, thus $C(K)$ is a group with identity $\mathcal{O}$, the point at infinity. Finally, since $a \notin K^3$ we can consider the derivation d/da of K.

THEOREM. *Let $\mu : C(K) \to K^+$ be defined by $\mu(\mathcal{O}) = 0$, $\mu((x,y)) = dy/da$. Then μ is an injective homomorphism. Further, there exists a divisor D of K with $\mu(C(K)) \subseteq L(D)$.*

PROOF: Let $P_i = (x_i, y_i) \in C(K), \quad i = 1,2,3$, satisfy $P_1 + P_2 + P_3 = 0$. Then P_1, P_2, P_3 are collinear, hence there exists $\alpha, \beta \in K$, $y_i = \alpha x_i + \beta, \quad i = 1,2,3$.

Received 30th March 1989

Therefore x_1, x_2, x_3 satisfy the equation $x^3 + a - (\alpha x + \beta)^2 = 0$, so $x_1 + x_2 + x_3 = \alpha^2$. It follows that

$$y_1 + y_2 + y_3 = \alpha(x_1 + x_2 + x_3) + 3\beta = \alpha^3.$$

Whence, applying d/da,

$$\mu(P_1) + \mu(P_2) + \mu(P_3) = 0.$$

It follows that μ is a homomorphism.

Differentiating the defining equation $y^2 = x^3 + a$, we get $2y dy/da = 1$, so $\mu(P) \neq 0$ for $P \neq \mathcal{O}$, and μ is injective.

Now, let v be a place of K and $P = (x, y) \in C(K)$. As $v(dy) \geqslant v(y) - 1$, we have $v(y) \leqslant v(\mu(P)) + v(da) + 1$. On the other hand $2y dy/da = 1$, so

$$v(\mu(P)) = -v(y) \geqslant -(v(\mu(P)) + v(da) + 1).$$

It follows that
$$v(\mu(P)) \geqslant -\frac{(v(da) + 1)}{2}.$$

If $v(da) = 0$, this of course improves to $v(\mu(P)) \geqslant 0$ and the result follows. $\square$

Remarks. (1) A similar behaviour to that observed above in characteristic 3 happens in characteristic 2 with Mordell's equation. More generally the equation $y^2 = x^3 + ax + b$, where a or b is not a square, is the most general curve in characteristic 2 of non-conservative genus 1, possessing a rational point. In fact this curve and Mordell's equation in characteristic 3 are the only such curves ([**3**]). We have also analogous results in this case taking $\mu(x, y) = dx/dt$ for some $t \in K \setminus K^2$. The theorem and its corollary hold in this case as well except for the fact that $\ker \mu = \{\mathcal{O}, (u, v)\}$, where $u = db/da$, if $a \notin K^2$. We leave the details to the reader.

(2) The map μ constructed above may seem rather mysterious but it is the analogue, in this situation, of Manin's map. (See [**5**]).

References

[1] C. Chevalley, *Introduction to the Theory of algebraic functions of one variable* (American Mathematical Society, New York, 1951).

[2] L.J. Mordell, *Diophantine Equations* (Academic Press, New York, 1969).

[3] C.S. Queen, 'Non-conservative function fields of genus one, I, II', *Arch. Math.* **22** (612-623). and **23** (1972) pp. 30–37.

[4] J.H. Silverman, *The Arithmetic of elliptic curves* (Springer, New York, 1986).

[5] J.F. Voloch, 'Explicit p-descent for elliptic curves in characteristic p', *Compositio Math.* (to appear).

IMPA
Estrada D. Castorina 110
Rio de Janeiro 22460 Brasil