



Universiteit  
Leiden  
The Netherlands

## **Diophantine equations in positive characteristic**

Koymans, P.H.

### **Citation**

Koymans, P. H. (2019, June 19). *Diophantine equations in positive characteristic*. Retrieved from <https://hdl.handle.net/1887/74294>

Version: Not Applicable (or Unknown)

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/74294>

**Note:** To cite this publication please use the final published version (if applicable).

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/74294> holds various files of this Leiden University dissertation.

**Author:** Koymans, P.H.

**Title:** Diophantine equations in positive characteristic

**Issue Date:** 2019-06-19

# Chapter 1

## The generalized Catalan equation in positive characteristic

### Abstract

Let  $K = \mathbb{F}_p(z_1, \dots, z_r)$  be a finitely generated field over  $\mathbb{F}_p$  and fix  $a, b \in K^*$ . We study the solutions of the generalized Catalan equation  $ax^m + by^n = 1$  to be solved in  $x, y \in K$  and integers  $m, n > 1$  coprime with  $p$ .

### 1.1 Introduction

In this article we will bound  $m$  and  $n$  for the generalized Catalan equation in characteristic  $p > 0$ . Our main result is as follows.

**Theorem 1.1.1.** *Let  $a, b \in K^*$  be given. Consider the equation*

$$ax^m + by^n = 1 \tag{1.1}$$

*in  $x, y \in K$  and integers  $m, n > 1$  coprime with  $p$  satisfying*

$$(m, n) \notin \{(2, 2), (2, 3), (3, 2), (2, 4), (4, 2), (3, 3)\}. \tag{1.2}$$

*Then there is a finite set  $\mathcal{T} \subseteq K^2$  such that for any solution  $(x, y, m, n)$  of (1.1), there is a  $(\gamma, \delta) \in \mathcal{T}$  and  $t \in \mathbb{Z}_{\geq 0}$  such that*

$$ax^m = \gamma^{p^t}, by^n = \delta^{p^t}. \tag{1.3}$$

In the case  $a = b = 1$ , a stronger and effective result was proven in [42] based on the work of [6].

Let us now show that the conditions on  $m$  and  $n$  are necessary. If (1.2) fails, then (1.1) defines a curve of genus 0 or 1 over  $K$ . It is clear that (1.3) can fail in this case. It is also essential that  $m$  and  $n$  are coprime with  $p$ . Take for example  $a = b = 1$ . Then any solution of

$$x + y = 1$$

with  $x, y \in K$  and  $x, y \notin \overline{\mathbb{F}_p}$  gives infinitely many solutions of the form (1.3) after applying Frobenius.

The generalized Catalan equation over function fields was already analyzed in [66], where the main theorem claims that the generalized Catalan equation has no solutions for  $m$  and  $n$  sufficiently large. Unfortunately, it is not hard to produce counterexamples to the main theorem given there. Following the notation in [66], we choose  $k = \mathbb{F}_p$ ,  $K = k(u)$ ,  $a = x = u$ ,  $b = y = 1 - u$  and  $m = n = p^t - 1$  for  $t \in \mathbb{Z}_{\geq 0}$ . Then we have

$$ax^m + by^n = u \cdot u^{p^t-1} + (1-u) \cdot (1-u)^{p^t-1} = 1$$

due to Frobenius, illustrating the need of (1.3).

## 1.2 Heights

Let  $K$  be a finitely generated extension of  $\mathbb{F}_p$ . The algebraic closure of  $\mathbb{F}_p$  in  $K$  is a finite extension of  $\mathbb{F}_p$ , say  $\mathbb{F}_q$  with  $q = p^n$  for some  $n \in \mathbb{Z}_{>0}$ . There exists a projective variety  $V$  non-singular in codimension one defined over  $\mathbb{F}_q$  with function field  $K$ .

Our goal will be to introduce a height function on  $K$  by using our variety  $V$ . For later purposes it will be useful to do this in a slightly more general setting. So let  $X$  be a projective variety, non-singular in codimension one, defined over a perfect field  $k$ . We write  $L$  for the function field of  $X$  and we assume that  $k$  is algebraically closed in  $L$ .

Fix a projective embedding of  $X$  such that  $X \subseteq \mathbb{P}_k^M$  for some positive integer  $M$ . Then a prime divisor  $\mathfrak{p}$  of  $X$  over  $k$  is by definition an irreducible subvariety of codimension one. Recall that for a prime divisor  $\mathfrak{p}$  the local ring  $\mathcal{O}_{\mathfrak{p}}$  is a discrete valuation ring, since  $X$  is non-singular in codimension one. Following [47] we will define heights on  $X$ . To do this, we start by defining a set of normalized discrete valuations

$$M_L := \{\text{ord}_{\mathfrak{p}} : \mathfrak{p} \text{ prime divisor of } X\},$$

where  $\text{ord}_{\mathfrak{p}}$  is the normalized discrete valuation of  $L$  corresponding to  $\mathcal{O}_{\mathfrak{p}}$ . If  $v = \text{ord}_{\mathfrak{p}}$  is in  $M_L$ , we define for convenience  $\deg v := \deg \mathfrak{p}$  with  $\deg \mathfrak{p}$  being the projective degree in  $\mathbb{P}_k^M$ . Then the set  $M_L$  satisfies the sum formula for all  $x \in L^*$

$$\sum_v v(x) \deg v = 0.$$

If  $P$  is a point in  $\mathbb{P}^r(L)$  with coordinates  $(y_0 : \dots : y_r)$  in  $L$ , then its (logarithmic) height is

$$h_L(P) = - \sum_v \min_i \{v(y_i)\} \deg v.$$

Furthermore we define for an element  $x \in L$

$$h_L(x) = h_L(1 : x). \quad (1.4)$$

We will need the following properties of the height.

**Lemma 1.2.1.** *Let  $x, y \in L$  and  $n \in \mathbb{Z}$ . The height defined by (1.4) has the following properties:*

$$(a) \quad h_L(x) = 0 \Leftrightarrow x \in k;$$

$$(b) \quad h_L(x + y) \leq h_L(x) + h_L(y);$$

$$(c) \quad h_L(xy) \leq h_L(x) + h_L(y);$$

$$(d) \quad h_L(x^n) = |n|h_L(x);$$

$$(e) \quad \text{Suppose that } k \text{ is a finite field and let } C > 0 \text{ be given. Then there are only finitely many } x \in L^* \text{ satisfying } h_L(x) \leq C;$$

$$(f) \quad h_L(x) = h_{\bar{k} \cdot L}(x).$$

*Proof.* Property (a) is Proposition 4 of [46] (p. 157), while properties (b), (c) and (d) are easily verified. Property (e) is proven in [55]. Finally, property (f) can be found after Proposition 3.2 in [47] (p. 63).  $\square$

## 1.3 A generalization of Mason's ABC-theorem

For our proof we will need a generalization of Mason's ABC-theorem for function fields in one variable to an arbitrary number of variables. Such a result is given in [36]. For completeness we repeat it here.

**Theorem 1.3.1.** *Let  $X$  be a projective variety over an algebraically closed field  $k$  of characteristic  $p > 0$ , which is non-singular in codimension one. Let  $L = k(X)$  be its function field and let  $M_L$  be as above. Let  $L_1, \dots, L_q$ ,  $q \geq n+1$ , be linear forms in  $n+1$  variables over  $k$  which are in general position. Let  $\mathbf{X} = (x_0 : \dots : x_n) \in \mathbb{P}^n(L)$  be such that  $x_0, \dots, x_n$  are linearly independent over  $K^{p^m}$  for some  $m \in \mathbb{N}$ . Then, for any fixed*

finite subset  $S$  of  $M_L$ , the following inequality holds:

$$\begin{aligned} & (q - n - 1)h(x_0 : \dots : x_n) \\ & \leq \sum_{i=1}^q \sum_{v \notin S} \deg v \min\{np^{m-1}, v(L_i(\mathbf{X})) - \min_{0 \leq j \leq n} \{v(x_j)\}\} \\ & \quad + \frac{n(n+1)}{2} p^{m-1} \left( C_X + \sum_{v \in S} \deg v \right), \end{aligned}$$

where  $C_X$  is a constant depending only on  $X$ .

*Proof.* This is the main theorem in [36]. □

## 1.4 Proof of Theorem 1.1.1

In this section we proof our main theorem.

*Proof of Theorem 1.1.1.* Let  $(x, y, m, n)$  be an arbitrary solution. Let us first dispose with the case  $ax^m \in \mathbb{F}_q$ . Then also  $by^n \in \mathbb{F}_q$ , so we simply add  $\mathbb{F}_q \times \mathbb{F}_q$  to  $\mathcal{T}$ . From now on we will assume  $ax^m \notin \mathbb{F}_q$  and hence  $by^n \notin \mathbb{F}_q$ . It follows that

$$h_K(ax^m), h_K(by^n) \neq 0,$$

so we may write

$$ax^m = \gamma^{p^t}, by^n = \delta^{p^s}$$

for some  $t, s \in \mathbb{Z}_{\geq 0}$  and  $\gamma, \delta \notin K^p$ . After substitution we get

$$\gamma^{p^t} + \delta^{p^s} = 1.$$

Extracting  $p$ -th roots gives  $t = s$  and hence

$$\gamma + \delta = 1. \tag{1.5}$$

Our goal will be to apply the main theorem of [36] to (1.5). Note that Theorem 1.3.1 requires that the ground field  $k$  is algebraically closed. But a constant field extension does not change the height by Lemma 1.2.1(f). Hence we can keep working with our field  $K$  instead of  $\overline{\mathbb{F}_p} \cdot K$ . Define the following three linear forms in two variables  $X, Y$

$$\begin{aligned} L_1 &= X \\ L_2 &= Y \\ L_3 &= X + Y. \end{aligned}$$

We apply Theorem 1.3.1 with our  $V$ , the above  $L_1, L_2, L_3$  and  $\mathbf{X} = (\gamma : \delta) \in \mathbb{P}^1(K)$ . We claim that  $\gamma$  and  $\delta$  are linearly independent over  $K^p$ . Suppose that there are  $e, f \in K^p$  such that

$$e\gamma + f\delta = 0.$$

Together with  $\gamma + \delta = 1$  we find that

$$0 = e\gamma + f\delta = e(1 - \delta) + f\delta = e + (f - e)\delta.$$

If  $e \neq f$ , then this would imply that  $\delta \in K^p$ , contrary to our assumptions. Hence  $e = f$ , but then we find

$$0 = e\gamma + f\delta = e$$

and we conclude that  $e = f = 0$  as desired.

We still have to choose the subset  $S$  of  $M_K$  to which we apply Theorem 1.3.1. First we need to make some preparations. From now on  $v$  will be used to denote an element of  $M_K$ . Define

$$\begin{aligned} N_0 &:= \{v : v(a) \neq 0 \vee v(b) \neq 0\} \\ N_1 &:= \{v : v(a) = 0, v(b) = 0, v(\gamma) > 0\} \\ N_2 &:= \{v : v(a) = 0, v(b) = 0, v(\delta) > 0\} \\ N_3 &:= \{v : v(a) = v(b) = 0, v(\gamma) = v(\delta) < 0\}. \end{aligned}$$

It is clear that  $N_0, N_1, N_2$  and  $N_3$  are finite disjoint sets. Before we proceed, we make a simple but important observation in the form of a lemma.

**Lemma 1.4.1.** *Let  $(\gamma, \delta)$  be a solution of (1.5). If  $v(\gamma) < 0$  or  $v(\delta) < 0$ , then*

$$v(\gamma) = v(\delta) < 0.$$

*Proof.* Obvious. □

Recall that

$$h_K(\gamma) = \sum_v \max(0, v(\gamma)) \deg v = \sum_v -\min(0, v(\gamma)) \deg v$$

and

$$h_K(\delta) = \sum_v \max(0, v(\delta)) \deg v = \sum_v -\min(0, v(\delta)) \deg v.$$

Lemma 1.4.1 tells us that

$$\sum_v -\min(0, v(\gamma)) \deg v = \sum_v -\min(0, v(\delta)) \deg v,$$

hence

$$h_K(\gamma) = h_K(\delta) = \sum_v \max(0, v(\gamma)) \deg v = \sum_v -\min(0, v(\gamma)) \deg v \quad (1.6)$$

$$= \sum_v \max(0, v(\delta)) \deg v = \sum_v -\min(0, v(\delta)) \deg v. \quad (1.7)$$

We will use these different expressions for the height throughout. Let us now derive elegant upper bounds for  $N_1, N_2$  and  $N_3$ . Again we will phrase it as a lemma.

**Lemma 1.4.2.** *Let  $(\gamma, \delta)$  be a solution of (1.5). Then*

$$\begin{aligned} h_K(\gamma) = h_K(\delta) &\geq m \sum_{v \in N_1} \deg v, \\ h_K(\gamma) = h_K(\delta) &\geq n \sum_{v \in N_2} \deg v, \\ h_K(\gamma) = h_K(\delta) &\geq \text{lcm}(m, n) \sum_{v \in N_3} \deg v. \end{aligned}$$

*Proof.* We know that

$$h_K(\gamma) = h_K(\delta) = \sum_v \max(0, v(\gamma)) \deg v \geq \sum_{v \in N_1} \max(0, v(\gamma)) \deg v.$$

Now let  $v \in N_1$ . This means that  $v(a) = v(b) = 0$  and  $v(\gamma) > 0$ . Then  $ax^m = \gamma^{p^t}$  implies

$$v(a) + mv(x) = p^t v(\gamma)$$

and hence  $mv(x) = p^t v(\gamma)$ . But  $m$  and  $p$  are coprime by assumption, so we obtain  $m \mid v(\gamma)$ . Because  $v(\gamma) > 0$ , this gives  $v(\gamma) \geq m$  and we conclude that

$$h_K(\gamma) = h_K(\delta) \geq m \sum_{v \in N_1} \deg v.$$

Using

$$h_K(\gamma) = h_K(\delta) = \sum_v \max(0, v(\delta)) \deg v \geq \sum_{v \in N_2} \max(0, v(\delta)) \deg v,$$

we find in a similar way that

$$h_K(\gamma) = h_K(\delta) \geq n \sum_{v \in N_2} \deg v.$$

It remains to be proven that

$$h_K(\gamma) = h_K(\delta) \geq \text{lcm}(m, n) \sum_{v \in N_3} \deg v.$$

Now we use

$$\begin{aligned} h_K(\gamma) = h_K(\delta) &= \sum_v -\min(0, v(\gamma)) \deg v = \sum_v -\min(0, v(\delta)) \deg v \\ &\geq \sum_{v \in N_3} -\min(0, v(\gamma)) \deg v = \sum_{v \in N_3} -\min(0, v(\delta)) \deg v. \end{aligned}$$

Now take  $v \in N_3$ . Then  $v(\gamma) = v(\delta) < 0$ . In the same way as before, we can show that  $m \mid v(\gamma)$  and  $n \mid v(\delta)$ . But  $v(\gamma) = v(\delta) < 0$  by Lemma 1.4.1, so we find that

$$h_K(\gamma) = h_K(\delta) \geq \text{lcm}(m, n) \sum_{v \in N_3} \deg v$$

as desired. □



Define

$$S := N_0 \cup N_1 \cup N_2 \cup N_3.$$

Suppose that  $v \notin S$ . We claim that

$$v(\gamma) = v(\delta) = 0.$$

But  $v \notin S$  implies  $v \notin N_0$ , so certainly  $v(a) = v(b) = 0$ . Furthermore, we have that  $v \notin N_1$  and  $v \notin N_2$ , which means that  $v(\gamma) \leq 0$  and  $v(\delta) \leq 0$ . If  $v(\gamma) < 0$  or  $v(\delta) < 0$ , then Lemma 1.4.1 gives  $v \in N_3$ , contradicting our assumption  $v \notin S$ . Hence  $v(\gamma) = v(\delta) = 0$  as desired.

From our claim it follows that we have for  $v \notin S$  and  $i = 1, 2, 3$

$$v(L_i(\gamma, \delta)) = \min(v(\gamma), v(\delta)).$$

Theorem 1.3.1 tells us that

$$h_K(\gamma : \delta) \leq C_W + \sum_{v \in S} \deg v,$$

where  $C_W$  is a constant depending on  $W$  only. By Lemma 1.4.2 we find that

$$\begin{aligned} \sum_{v \in S} \deg v &= \sum_{v \in N_0} \deg v + \sum_{v \in N_1} \deg v + \sum_{v \in N_2} \deg v + \sum_{v \in N_3} \deg v \\ &\leq C_{a,b} + \left( \frac{1}{m} + \frac{1}{n} + \frac{1}{\text{lcm}(m, n)} \right) h_K(\gamma), \end{aligned}$$

where  $C_{a,b}$  is a constant depending on  $a$  and  $b$  only. Now (1.2) implies

$$\frac{1}{m} + \frac{1}{n} + \frac{1}{\text{lcm}(m, n)} < 0.9,$$

hence

$$h_K(\gamma : \delta) \leq 10(C_W + C_{a,b}).$$

But  $\gamma + \delta = 1$  gives

$$h_K(\gamma) = h_K(\delta) = h_K(\gamma : \delta).$$

The theorem now follows from Lemma 1.2.1(e). □

## 1.5 Discussion of Theorem 1.1.1

The conclusion of Theorem 1 tells us that there is a finite set  $\mathcal{T} \subseteq K^2$  such that for any solution  $(x, y, m, n)$  of (1.1), there is a  $(\gamma, \delta) \in \mathcal{T}$  and  $t \in \mathbb{Z}_{\geq 0}$  such that

$$ax^m = \gamma^{p^t}, by^n = \delta^{p^t}.$$

Since  $\mathcal{T}$  is finite, we may assume that  $\gamma$  and  $\delta$  are fixed in the above two equations. It would be interesting to further study this equation.

