REMARKS ON CATALAN'S EQUATION OVER FUNCTION FIELDS

ANWESH RAY

ABSTRACT. Let ℓ be a prime number, F be a global function field of characteristic ℓ. Assume that there is a prime P_∞ of degree 1. Let $\mathcal{O}_F$ be the ring of functions in F with no poles other than P_∞. We study solutions to Catalan's equation $X^m - Y^n = 1$ over $\mathcal{O}_F$ and show that under certain additional conditions, there are no non-constant solutions which lie in $\mathcal{O}_F$.

1. INTRODUCTION

Let $m > 1$ and $n > 1$ be integers, and consider the diophantine equation

$$X^m - Y^n = 1.$$

The famous Catalan conjecture states that there are no non-trivial integer solutions to the above equation except when $m = 2$, $n = 3$ and $(X, Y) = (\pm 3, 2)$. The celebrated result of Mihăilescu resolves this conjecture using techniques from the theory of cyclotomic fields (cf. [Mih04]). Given the close analogy between number fields and function fields, it is of interest to study analogues of Catalan's conjecture in characteristic $\ell > 0$. The field of rational numbers $\mathbb{Q}$ is the simplest number field to consider, and analogously, the most natural analogue is the field of rational functions $\mathbb{F}(T)$, where T is a formal variable, and $\mathbb{F}$ is a finite field. The ring of integers $\mathbb{Z}$ is thus analogous to the ring of polynomial functions $\mathbb{F}[T]$, which shares similar properties to $\mathbb{Z}$. The reader is referred to [Ros02, Gol06] for an introduction to the arithmetic of function fields, and further perspectives elaborating the close analogy between number fields and their counterparts in positive characteristic.

Let ℓ be a prime number and F be a global function field of characteristic ℓ. Denote by $\mathbb{F}_\ell$ the finite field with ℓ elements and set κ to denote the algebraic closure of $\mathbb{F}_\ell$ in F. Note that κ is a finite field (by assumption). Recall (from [Ros02, Chapter 5]) that a *prime* in F is defined to be the maximal ideal v of a discrete valuation ring R contained in F, with fraction field equal to F. Thus each prime v comes equipped with a valuation $\mathrm{ord}_v : F \to \mathbb{Z} \cup \{\infty\}$. Note that according to this description, there is no zero prime, since we do not consider F itself to be a discrete valuation ring. Assume that there exists a prime P_∞ of F which has degree 1, and let $\mathcal{O}_F$ be the ring of functions in F with no poles outside $\{P_\infty\}$. The point P_∞ is referred to as the *point at infinity* and $\mathcal{O}_F$ is the *ring of integers* of F. We say that a solution $(X, Y) \in \mathcal{O}_F^2$ to $X^m - Y^n = 1$ is *constant* if X and Y are both contained in κ, and *non-constant* otherwise.

Key words and phrases. Catalan's equation, Catalan's conjecture, function field arithmetic, diophantine equations over global function fields, Picard groups of projective curves.

Recall from *loc. cit.* that a divisor is a finite integral linear combination of primes of F. The principal divisor associated to $g \in F$ is denoted $\mathrm{div}(g)$, and two divisors D_1 and D_2 are said to be equivalent if $D_1 - D_2$ is a principal divisor. The group of divisors classes of degree 0 is finite (cf. [Ros02, Lemma 5.6]), and its cardinality is the *class number of* F, and this quantity is denoted by h_F. Given a prime number $p \neq \ell$, let $F(\mu_p)$ be the function field obtained by adjoining the p-th roots of unity μ_p to F. Note that $F(\mu_p) = \kappa' \cdot F$, where $\kappa' = \kappa(\mu_p)$. Thus, $F(\mu_p)$ is a constant field extension of F in the sense of [Ros02, Chapter 8].

Theorem 1.1. *Let F be a global function field of characteristic $\ell > 0$. Let p and q be prime numbers and assume that all the following conditions are satisfied*

(1) $p \neq \ell$ and $q \neq \ell$,
(2) if $p \neq q$, then, either $q \nmid h_{F(\mu_p)}$ or $p \nmid h_{F(\mu_q)}$.
(3) if $q = 2$, $p \neq 2$ and $q \mid h_{F(\mu_p)}$, then $p \nmid h_{F(\mu_4)}$.

Then, there are no non-constant solutions to $X^p - Y^q = 1$ in $\mathcal{O}_F$.

Thus, if m is divisible by a prime p and n by a prime q for which the above conditions are satisfied, then, there are no non-constant solutions to $X^m - Y^n = 1$ in $\mathcal{O}_F$. The condition requiring that p and q are distinct from ℓ is necessary, since if $m = \ell$ for instance, it is easy to construct a large class of non-constant solutions if one of primes is equal to ℓ (cf. Remark 2.3 for details).

We mention some related work of relevance. Silverman [Sil82] considered a general class of equations of the form $aX^m + bY^n = c$ over a general function field K, and proved that under some further conditions, there are only finitely many solutions when $a, b, c \in K^*$ are fixed. We refer to the work of Koymans [Koy22], where a correction is made to an argument in *loc. cit.* and the results are generalized to fields of larger dimension. The Catalan equation was studied by Nathanson [Nat74] over $K[T]$ and $K(T)$ where K is a field of positive characteristic. It is shown in *loc. cit.* that if $m > 2$ and $n > 2$ are coprime to ℓ then there are no solutions to Catalan's equation $X^m - Y^n = 1$ that lie in $K[T]$ but not in K. Specializing to the case when K is a finite field, one obtains the conclusion of Theorem 1.1 for the rational function field with the added stipulation that $m, n > 2$. This is because the class number of any rational function field is equal to 0. Theorem 1.1 can thus be viewed as a generalization of Nathanson's result to general function fields F with added stipulations on (m, n).

1.1. **Acknowledgment:** The author thanks Peter Koymans for a helpful suggestion.

2. Proof of the main result

Recall that F is a global function field of characteristic $\ell > 0$ with field of constants κ. Let $\bar{\kappa}$ be the algebraic closure of κ in a fixed algebraic closure of F, and set F' to denote the composite $F \cdot \bar{\kappa}$. Also, denote by A the composite $\mathcal{O}_F \cdot \bar{\kappa}$. The field F' is identified with the function field of a projective curve

$\mathfrak{X}$ over $\bar{\kappa}$ and each point in $\mathfrak{X}(\bar{\kappa})$ corresponds to a valuation ring $R \subset F'$ with residue field $\bar{\kappa}$ and fraction field F'. The valuation ring associated to $w \in \mathfrak{X}(\bar{\kappa})$ is denoted $\mathcal{O}_w$, and refer to w as a *prime of* F'. We say that w divides (or lies above) a prime v of F if there is a natural inclusion of valuation rings $\mathcal{O}_v \hookrightarrow \mathcal{O}_w$ induced by the inclusion $F \hookrightarrow F'$. Note that since P_∞ has degree 1, it is totally inert in F'. In particular, there is a single prime of F' that lies above P_∞, and we shall denote this prime by $\widetilde{P}_\infty$. Given any prime v of F, set d_v to denote $-\operatorname{ord}_v$ and for any function $g \in F$, we refer to $d_v(g)$ as the order of the pole of g at v. Given a prime w of F' (i.e., point $w \in \mathfrak{X}(\bar{\kappa})$) and $g \in F'$, denote by $d_w(g)$ the order of the pole of g at w. We set $d : A \to \mathbb{Z}_{\geq 0}$ to denote $d_{\widetilde{P}_\infty}$.

Lemma 2.1. *Let $f, g \in A$ be non-zero. The following assertions hold.*

(1) $d(g) = 0$ if and only if g is a constant function.
(2) We have that $d(fg) = d(f) + d(g)$.
(3) Suppose that $d(f) < d(g)$. Then, $d(g + f) = d(g)$.

Proof. Suppose that $d(g) = 0$ for a function $g \in A$, then g has no poles and it follows that g is constant (cf. [Gol06, Chapter 2]). The converse to this statement is clear, and thus we have proven (1).

It is clear that $\operatorname{ord}_w(fg) = \operatorname{ord}_w(f) + \operatorname{ord}_w(g)$ for any point $w \in \mathfrak{X}(\bar{\kappa})$ and (2) follows from this.

Since $d(f) < d(g)$, we have that f/g vanishes at P_∞, and hence, $d(1+f/g) = 0$. From part (2), we find that

$$d(g + f) = d(g) + d\left(1 + f/g\right) = d(g).$$

This proves part (3). □

Lemma 2.2. *Let $Y \in A$ and $c_1, c_2 \in \bar{\kappa}$ be non-zero constants. If for some prime $p \neq \ell$ we have that*

$$(Y + c_1)^p - Y^p = c_2,$$

then, Y is a constant.

Proof. Suppose that by way of contradiction that Y is not a constant, then, it must have a pole. Since $Y \in A$ by assumption, it can only have poles at $\widetilde{P}_\infty$. Suppose by way of contradiction that $d(Y) > 0$. We then have that

$$(Y + c_1)^p - Y^p = \sum_{i=1}^{p} \binom{p}{i} c_1^i Y^{p-i} = c_2. \tag{2.1}$$

We find that $d(Y^{p-i}) < d(Y^{p-1})$ for all $i > 1$. Noting that $p \neq \ell$, Lemma 2.1 part (3) implies that

$$d\left(\sum_{i=1}^{p} \binom{p}{i} c_1^i Y^{p-i}\right) = d(pc_1 Y^{p-1}) = (p-1)d(Y) > 0.$$

On the other hand, (2.1) implies then that $(p-1)d(Y) = d(c_2) = 0$, a contradiction. Hence, Y must be a constant function.

□

Proof of Theorem 1.1. First consider the case when $p = q$. Note that it is assumed that $p \neq \ell$. We show that there are no non-constant solutions to

$$X^p - Y^p = 1$$

in A. Note that $(X - Y)$ divides $X^p - Y^p = 1$, hence $d(X - Y) \leq d(1) = 0$. It follows from Lemma 2.1 part (1) that $(X - Y)$ is a constant $c \in \bar{\kappa}$. We thus deduced that

$$(Y + c)^p - Y^p = 1. \tag{2.2}$$

Lemma 2.2 implies that (2.2) has no nonconstant solutions. Since Y is a constant, it follows that X is as well. If X and Y are in $\mathcal{O}_S$, it follows therefore that $X, Y \in \kappa$.

We assume therefore that p and q are distinct (and distinct from ℓ). Note that there are further conditions on p and q. First, we consider the case when $q \nmid h_{F(\mu_p)}$. Let ζ be a primitive p-th root of 1 in κ. Since it is assumed that $p \neq \ell$, we note that $\zeta \neq 1$.

In what follows we consider divisors over $F(\mu_p)$. Given a divisor $D = \sum_v n_v v$ involving primes v of $F(\mu_p)$, the support consists of all primes v such that the coefficient n_v is not equal to 0. Factor $X^p - 1$ into linear factors to obtain the following equation

$$Y^q = \prod_{j=0}^{p-1} (X - \zeta^j). \tag{2.3}$$

For $i \neq j$, note that $(X - \zeta^i) - (X - \zeta^j) = \zeta^j - \zeta^i$, which is a non-zero element of $\kappa(\mu_p)$. Hence, it follows that $\operatorname{div}(X - \zeta^i)$ and $\operatorname{div}(X - \zeta^j)$ have disjoint supports for $i \neq j$. From (2.3), we have that

$$\sum_{j=0}^{p-1} \operatorname{div}(X - \zeta^j) = q \operatorname{div}(Y),$$

and since the divisors $\operatorname{div}(X - \zeta^j)$ have disjoint supports for $i \neq j$, it follows that for each i, there is a divisor D_i such that $\operatorname{div}(X - \zeta^i) = qD_i$. Since $\operatorname{div}(X - \zeta^i)$ is a principal divisor, it has degree 0, and hence D_i does also have degree zero. Since $q \nmid h_{F(\mu_p)}$, there is no non-trivial q torsion in the divisor class group. As a result, D_i is a principal divisor $\operatorname{div}(\alpha_i)$, where $\alpha_i \in F(\mu_p)$. Thus, we have deduced that for all i,

$$X - \zeta^i = u_i \alpha_i^q,$$

where u_i is a unit in $F(\mu_p)$ and hence in $\kappa(\mu_p)$. Note that u_i is the q-th power of an element $v_i \in \bar{\kappa}^\times$. Replacing α_i with $v_i \alpha_i$, we write

$$(X - \zeta^i) = \alpha_i^q,$$

where $\alpha_i \in (F')^\times$. Note that α_i is contained in A since it has no poles outside $\{\widetilde{P}_\infty\}$ (since $X - \zeta^i$ does not). We deduce that

$$\alpha_0^q - \alpha_1^q = (X - 1) - (X - \zeta) = \zeta - 1. \tag{2.4}$$

It follows that $\alpha_0 - \alpha_1$ divides $\zeta - 1$, hence has no zeros or poles. As a result, $\alpha_0 - \alpha_1$ is a constant $c \in \bar{\kappa}$. It is clear from (2.4) that c is non-zero. Thus we find that

$$(\alpha_1 + c)^q - \alpha_1^q = \zeta - 1.$$

Lemma 2.2 then implies that α_1 and α_0 are constants. We have thus shown that X, and hence Y are both elements in $\bar{\kappa}$. Since κ is the algebraic closure of $\mathbb{F}_\ell$ in F, and both X and Y are contained in F, it follows that $X, Y \in \kappa$.

Next, assume that $p \nmid h_{F(\mu_q)}$. If both p and q are odd, then we may replace X with $-Y$ and Y with $-X$ to obtain the equation $X^q - Y^p = 1$, and thus the previous argument gives the result applies in this case. Thus, we are left to consider the case when either p or q is 2.

First consider the case when $p = 2$ and $p \nmid h_{F(\mu_q)}$. Then, we find that $X^2 = Y^q + 1 = Y^q - (-1)^q = \prod_j (Y + \zeta^j)$, where ζ is a q-th root of unity. An identical argument to the previous case gives the result.

Finally, assume that p is odd, $p \nmid h_{F(\mu_4)}$ and $q = 2$. We consider the equation $X^p = Y^2 + 1 = (Y + \eta)(Y - \eta)$, where $\eta^2 = -1$. Note that $F(\mu_4) = F(\eta)$. Since p does not divide the class number of $F(\eta)$, we find that $Y + \eta = \alpha_0^p$ and $Y - \eta = \alpha_1^p$, where α_0, α_1 are elements in A. Therefore, $2\eta = \alpha_0^p - \alpha_1^p$. In particular, this implies that $(\alpha_0 - \alpha_1)$ is a non-zero constant c, and we have the following equation

$$(\alpha_1 + c)^p - \alpha_1^p = 2\eta.$$

The result follows from Lemma 2.2. □

Remark 2.3. At this point, it is pertinent to make a few remarks.

- In the proof of the above result, the assumptions $p \neq \ell$ and $q \neq \ell$ are crucially used at various points. To deduce that $1 - \zeta \neq 0$, it is necessary that $p \neq \ell$, otherwise, the factorization of $X^p - 1$ would simply be $(X - 1)^\ell$. The assumption that $q \neq \ell$ is also crucially used, especially in the last step, where it is shown that α_1 is a constant.
- The assumptions that p and q are not equal to ℓ are necessary. Indeed, suppose that $p = \ell$. Then, setting $X = 1 + z^q$ and $Y = z^p$ for any element $z \in \mathcal{O}_F$, one would obtain non-constant solutions.
- The methods introduced in this paper could potentially be applied to a more general class of diophantine equations, namely, equations of the form $X^m = f(Y)$, where $f(Y) \in \kappa[Y]$, where κ is the field of constants of F.

References

[Gol06] David Goldschmidt. *Algebraic functions and projective curves*, volume 215. Springer Science & Business Media, 2006.

[Koy22] Peter Koymans. The generalized Catalan equation in positive characteristic. *International Journal of Number Theory*, 18(02):269–276, 2022.

[Mih04] Preda Mihailescu. Primary cyclotomic units and a proof of Catalans conjecture. 2004.

[Nat74] Melvyn B Nathanson. Catalan's equation in k (t). *The American Mathematical Monthly*, 81(4):371–373, 1974.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2002.

[Sil82] Joseph H Silverman. The Catalan equation over function fields. *Transactions of the American Mathematical Society*, 273(1):201–205, 1982.

(A. Ray) Department of Mathematics, University of British Columbia, Vancouver BC, Canada V6T 1Z2

Email address: anweshray@math.ubc.ca