On the equation $\alpha\xi^m = \gamma^{p^t}$

Peter Koymans
p.h.koymans@math.leidenuniv.nl

February 15, 2016

The goal of this article is to analyze an equation that arises naturally in the study of the generalized Catalan equation in positive characteristic, see [1].

Setup
Let K be a finitely generated field over $\mathbb{F}_q$ with q a power of some prime $p > 0$. We assume that $\mathbb{F}_q$ is algebraically closed in K. Fix $\alpha, \gamma \in K^*$ and consider the equation

$$\alpha\xi^m = \gamma^{p^t} \tag{1}$$

with $\xi \in K^*$ and $m, t \in \mathbb{Z}_{\geq 0}$. We say that $t \in \mathbb{Z}_{\geq 0}$ is m-admissible if there is $\xi \in K^*$ such that (ξ, m, t) is a solution of (1). Define

$$\Gamma := \langle \alpha, \gamma \rangle$$

to be the multiplicative group generated by α and γ.

Theorem 1. *Suppose that $rk(\Gamma) = 2$. Then there are only finitely many possibilities for m. Furthermore, for each fixed m the set of m- admissible t is empty or an arithmetic progression.*

Proof. Define

$$\Gamma' := \{x \in K^* : \exists m > 0 \text{ such that } x^m \in \Gamma\}.$$

Because K and Γ are finitely generated, it follows that Γ' is finitely generated too. Recall that $\mathbb{F}_q$ was algebraically closed in K. It follows that $\Gamma^{\text{tors}} = \Gamma \cap \mathbb{F}_q^*$ and that $\Gamma'^{\text{tors}} = \mathbb{F}_q^*$. Hence we get that

$$\Gamma/(\Gamma \cap \mathbb{F}_q^*) \trianglelefteq \Gamma'/\mathbb{F}_q^*,$$

where $\Gamma'/\mathbb{F}_q^*$ is a finitely generated free abelian group. So we can find a basis $\gamma_1, \dots, \gamma_r$ of $\Gamma'/\mathbb{F}_q^*$ such that

$$\Gamma'/\mathbb{F}_q^* = \langle \gamma_1, \dots, \gamma_r \rangle$$
$$\Gamma/(\Gamma \cap \mathbb{F}_q^*) = \langle \gamma_1^{d_1}, \dots, \gamma_{r'}^{d_{r'}} \rangle$$

for some $r' \leq r$, $d_1 \mid \dots \mid d_{r'}$.

Then, using the definition of Γ' and our assumption that $\text{rk}(\Gamma) = 2$, it follows that $r = r' = 2$. We conclude that

$$\Gamma'/\mathbb{F}_q^* = \langle \gamma_1, \gamma_2 \rangle.$$

So we can write uniquely

$$\Gamma' = \{\zeta^{m_0}\gamma_1^{m_1}\gamma_2^{m_2} : m_0 \in \{0, \dots, q-2\}, m_1, m_2 \in \mathbb{Z}\}$$

with ζ a primitive element of $\mathbb{F}_q^*$. Observe that $\xi \in \Gamma'$, so we can write

$$\begin{aligned} \alpha &= \zeta^{a_0}\gamma_1^{a_1}\gamma_2^{a_2} \\ \gamma &= \zeta^{c_0}\gamma_1^{c_1}\gamma_2^{c_2} \\ \xi &= \zeta^{x_0}\gamma_1^{x_1}\gamma_2^{x_2} \end{aligned}$$

with $a_0.c_0, x_0 \in \{0, \ldots, q-2\}$ and $a_i, c_i, x_i \in \mathbb{Z}$ for $i = 1, 2$. Then (ξ, m, t) is a solution to (1) if and only if

$$\begin{aligned} a_0 + mx_0 &\equiv p^t c_0 \mod (q-1) \\ a_1 + mx_1 &= p^t c_1 \\ a_2 + mx_2 &= p^t c_2. \end{aligned} \tag{2}$$

Our assumption $\mathrm{rk}(\Gamma) = 2$ tells us that $a_1c_2 \neq a_2c_1$. Write $m = p^s m'$ with $p \nmid m'$. We claim that there are only finitely many options for s and m', hence for m. But indeed

$$m(a_2x_1 - a_1x_2) = p^t(a_2c_1 - a_1c_2),$$

so $m' \mid a_2c_1 - a_1c_2$. Since $a_2c_1 - a_1c_2 \neq 0$, this gives finitely many possibilities for m'.

Now we are going to bound s and for this we note that $a_1 \neq 0$ or $a_2 \neq 0$, again by the fact that $a_1c_2 \neq a_2c_1$. Suppose without loss of generality that $a_1 \neq 0$. The equation $a_1 + mx_1 = p^t c_1$ implies

$$p^{\min(s,t)} \mid a_1,$$

so $\min(s, t)$ is bounded. On the other hand recall that

$$m \mid p^t(a_2c_1 - a_1c_2),$$

which implies that $s \leq t + \mathrm{ord}_p(a_2c_1 - a_1c_2)$. This shows that s is bounded, which completes the proof of the first part of Theorem 1.

So from now on we assume that m', s and hence m are fixed. If (ξ, t) is a solution to (2), then t satisfies

$$\begin{aligned} a_0 &\equiv p^t c_0 \mod \gcd(m, q-1) \\ a_1 &\equiv p^t c_1 \mod m \\ a_2 &\equiv p^t c_2 \mod m. \end{aligned} \tag{3}$$

Reversely, if t satisfies (3), then (ξ, t) satisfies (2) for a uniquely determined ξ. Therefore it suffices to analyze (3). By the Chinese remainder theorem (3) is the same as

$$\begin{aligned} a_0 &\equiv p^t c_0 \mod \gcd(m, q-1) \\ a_1 &\equiv p^t c_1 \mod m' \\ a_2 &\equiv p^t c_2 \mod m' \\ a_1 &\equiv p^t c_1 \mod p^s \\ a_2 &\equiv p^t c_2 \mod p^s. \end{aligned} \tag{4}$$

First we look at the first three equations of (4). If there is no solution $t \in \mathbb{Z}_{\geq 0}$, then the set of m-admissible t is empty. So for the remainder of this article we assume that there is a solution $t \in \mathbb{Z}_{\geq 0}$. Let t_0 be the smallest solution and let t be any solution. Then the first three equations can be rewritten as

$$\begin{aligned} p^t c_0 &\equiv p^{t_0} c_0 \mod \gcd(m, q-1) \\ p^t c_1 &\equiv p^{t_0} c_1 \mod m' \\ p^t c_2 &\equiv p^{t_0} c_2 \mod m', \end{aligned}$$

which is equivalent to

$$\begin{aligned} p^{t-t_0} &\equiv 1 \mod \frac{\gcd(m, q-1)}{\gcd(m, q-1, c_0)} \\ p^{t-t_0} &\equiv 1 \mod \frac{m'}{\gcd(c_1, m')} \\ p^{t-t_0} &\equiv 1 \mod \frac{m'}{\gcd(c_2, m')}. \end{aligned} \tag{5}$$

Define

$$\begin{aligned} O_1 &:= \text{ order of } p \text{ in } \left(\mathbb{Z}/\frac{\gcd(m, q-1)}{\gcd(m, q-1, c_0)}\mathbb{Z}\right)^* \\ O_2 &:= \text{ order of } p \text{ in } \left(\mathbb{Z}/\frac{m'}{\gcd(c_1, m')}\mathbb{Z}\right)^* \\ O_3 &:= \text{ order of } p \text{ in } \left(\mathbb{Z}/\frac{m'}{\gcd(c_2, m')}\mathbb{Z}\right)^*. \end{aligned}$$

Then t satisfies the first equation of (5) if and only if

$$t = t_0 + nO_1$$

for some $n \in \mathbb{Z}_{\geq 0}$ and similarly for the second and third equation. Hence t satisfies (5) if and only if

$$t = t_0 + n\mathrm{lcm}(O_1, O_2, O_3)$$

for some $n \in \mathbb{Z}_{\geq 0}$.

We still need to study the last two equations of (4), i.e.

$$\begin{aligned} a_1 &\equiv p^t c_1 \mod p^s \\ a_2 &\equiv p^t c_2 \mod p^s. \end{aligned} \tag{6}$$

We distinguish two cases. If $a_1 \equiv a_2 \equiv 0 \mod p^s$, then t satisfies (6) if and only if $t \geq s - \mathrm{ord}_p(c_2)$. We conclude that in this case t satisfies (4) if and only if $t = t_0 + n\mathrm{lcm}(O_1, O_2, O_3)$ for some $n \in \mathbb{Z}_{\geq 0}$ and $t \geq s - \mathrm{ord}_p(c_2)$. Clearly, the $t \in \mathbb{Z}_{\geq 0}$ satisfying these two conditions form an arithmetic progression as desired.

Suppose instead without loss of generality that $a_1 \not\equiv 0 \mod p^s$. Then the equation

$$a_1 \equiv p^t c_1 \mod p^s$$

can have at most one solution $t \in \mathbb{Z}_{\geq 0}$. Hence (4) has either a single or no solution. Again we reach the desired conclusion, which completes the proof of Theorem 1. □

Discussion

The case $\mathrm{rk}(\Gamma) = 1$ leads to slightly different behavior. It is easy to see that the first part of Theorem 1 no longer holds. Indeed, take $K = \mathbb{F}_p(u)$ over $\mathbb{F}_p$. Choose $\alpha = \gamma = u$, then we have

$$u \cdot u^{p^t - 1} = u^{p^t}$$

for all $t \in \mathbb{Z}_{\geq 0}$.

Define t to be admissible if it is m-admissible for some $m \geq 2$. Then t is admissible if and only if there is $m \in \mathbb{Z}_{\geq 2}$ such that $m \mid p^t c_1 - a_1$ and $\gcd(m, q-1) = 1$. Then, using results on S-unit equations (see Mahler), one can show that t is admissible for all sufficiently large t.

References

[1] P. Koymans (2015), *The generalized Catalan equation in positive characteristic,* `http://pub.math.leidenuniv.nl/~koymansph/CatalanFinalResult2.pdf`