Trends in Mathematics
Information Center for Mathematical Sciences
Volume 9, Number 2, December, 2006, Pages 113–117

ON SCHINZEL'S HYPOTHESIS IN POSITIVE CHARACTERISTICS

ANDREAS O. BENDER

1. Introduction

The Schinzel hypothesis over Z: Let $f_1(x), \ldots, f_r(x)$ be irreducible polynomials with coefficients in $\mathbf{Z}$. Assume that the leading coefficient of every $f_i(x)$ is positive and that for each prime p, there exists an integer x_p such that no $f_i(x_p)$ is divisible by p. Then $f_1(x), \ldots, f_r(x)$ are simultaneously prime for infinitely many integer values of x ([6]).

The Schinzel hypothesis over $\mathbf{F}_q[t]$: There is a naïve analogon to the Schinzel hypothesis over the coefficient ring $\mathbf{F}_q[t]$ rather than $\mathbf{Z}$.

This analogous hypothesis is known to be false, a counterexample being the following: Let $f(X) = X^{4q} + t^{2q-1}$. Then $f(g)$ is reducible for all $g \in \mathbf{F}_q[t]$ (see [3, Section 3]).

The result we are going to discuss in the rest of this note is the following

Theorem 1.1. *Let $\mathbf{F}_q$ be a finite field of characteristic p and cardinality q. Let $f_1, \ldots, f_n \in \mathbf{F}_q[t, x]$ be irreducible polynomials whose total degrees $\deg(f_i)$ satisfy $p \nmid \deg(f_i)(\deg(f_i) - 1)$ for all i. Assume that the curves $C_i \subseteq \mathbf{P}^2_{\mathbf{F}_q}$ defined as the Zariski closures of the affine curves*

$$f_i(x, t) = 0$$

are smooth. Then, for any sufficiently large $s \in \mathbf{N}$, there exist $a, b \in \mathbf{F}_{q^s}$ such that the polynomials $f_1(at + b, t), \ldots, f_n(at + b, t) \in \mathbf{F}_{q^s}[t]$ are all irreducible.

Acknowledgements: This note is an abridged version of the joint paper [1] of the author with Olivier Wittenberg, where the full proof of theorem 1.1 can be found.

Notations. We denote by $|S|$ the cardinality of a set S and by $\mathfrak{S}(S)$ the symmetric group on S. Let k be a field and X be a k-scheme. If k' is a field extension of k, the scheme $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k')$ will often be denoted $X_{k'}$. We write $\kappa(x)$ for the residue field of $x \in X$, and $\kappa(X)$ for the function field of X when X is integral. Finally, when Y is an X-scheme, $\mathrm{Aut}_X(Y)$ denotes the group of X-automorphisms of Y.

2. A preliminary result about generic covers of $\mathbf{P}^1$

If k is a field, a finite k-scheme X will be said to have *at most one double point* if $n(X) \geq r(X) - 1$, where $r(X)$ and $n(X)$ respectively denote the rank and the geometric number of points of X.

Definition 2.1. *A finite morphism $f\colon C \to \mathbf{P}^1_k$ is called generic if $f^{-1}(x)$ has at most one double point for all $x \in \mathbf{P}^1_k$.*

Proposition 2.2. *Let C be a regular, complete, geometrically irreducible curve over a field k, endowed with a finite separable generic morphism $f\colon C \to \mathbf{P}^1_k$. Let C' be a regular, complete, irreducible curve over k, and $g\colon C' \to C$ be a finite morphism. Assume that the finite extension $\kappa(C')/\kappa(\mathbf{P}^1_k)$ is a Galois closure of the subextension $\kappa(C)/\kappa(\mathbf{P}^1_k)$. We denote respectively by G and H the Galois groups of $\kappa(C')/\kappa(\mathbf{P}^1_k)$ and $\kappa(C')/\kappa(C)$. Then C' is geometrically irreducible over k and the morphism*

$$G \longrightarrow \mathfrak{S}(H\backslash G)$$

induced by right multiplication is an isomorphism. Moreover, all the ramification indices of $\kappa(C')/\kappa(\mathbf{P}^1_k)$ are ≤ 2.

Sketch of proof: At first, one establishes a setup in which irreducibility, geometric irreducibility and the respective Galois groups can be considered. Let k' denote the algebraic closure of k in $\kappa(C')$. We denote respectively by G' and H' the subgroups of G defined by the subfields $\kappa(\mathbf{P}^1_{k'})$ and $\kappa(C_{k'})$ of $\kappa(C')$. It turns out that it suffices to consider G'.

Then the main tools is

Lemma 2.3. *Let X be a regular, complete, geometrically irreducible curve over a field K, endowed with a finite and generically Galois morphism $X \to \mathbf{P}^1_K$ with group G. Then G is generated by the inertia subgroups above closed points of $\mathbf{P}^1_K$ and their conjugates.*

A very similar lemma is stated and proved in [7, Proposition 4.4.6].

Let us consider the cover $C' \to \mathbf{P}^1_{k'}$. It is generically Galois with group G'. Let $I \subseteq G'$ be the inertia subgroup of G' associated with a point of C' whose image by $f \circ g$ will be denoted x. By Lemma 4.1, the geometric number of points of $f^{-1}(x)$ is $|H'\backslash G'/I|$. Moreover, the rank of $f^{-1}(x)$ is $|H'\backslash G'|$. The hypothesis that $f^{-1}(x)$ has at most one double point thus leads to the inequality

$$|H'\backslash G'/I| \geq |H'\backslash G'| - 1,$$

thereby proving that every non-trivial inertia subgroup of G' has order 2 and acts by a transposition on $H'\backslash G'$. Applying Lemma 2.3 to $X = C'$ and $K = k'$ now yields that G' is generated by elements which act on $H'\backslash G'$ by transpositions. The image of $G' \to \mathfrak{S}(H'\backslash G')$ is therefore a transitive subgroup of $\mathfrak{S}(H'\backslash G')$ which is generated by transpositions; but the only such subgroup is $\mathfrak{S}(H'\backslash G')$ itself (see [7, Lemma 4.4.4]), hence the result. □

3. Proof of Theorem 1.1

We may assume that the polynomials $(f_i)_{1\leq i\leq n}$ are pairwise non-proportional. Let $\mathbf{F}$ denote an algebraic closure of $\mathbf{F}_q$. The symbol $\mathbf{F}_{q^s}$ will now be understood to refer to the unique subfield of $\mathbf{F}$ with cardinality q^s. Let $M_0 \in \mathbf{P}^2(\mathbf{F}_q)$ denote the point at infinity with coordinates $x = 1$, $t = 0$.

Proposition 3.1. *There exists a non-empty open subset $U \subset \mathbf{P}^2_{\mathbf{F}_q} \setminus \{M_0\}$, disjoint from C_i for all $i \in \{1, \ldots, n\}$, such that every line D in $\mathbf{P}^2_{\mathbf{F}}$ which meets U satisfies the following properties:*

1. *For all $i \in \{1, \ldots, n\}$, the scheme-theoretic intersection $(C_i)_{\mathbf{F}} \cap D$ has at most one double point (as a finite $\mathbf{F}$-scheme).*
2. *The line D is not tangent to more than one of the curves $(C_i)_{\mathbf{F}}$, $i \in \{1, \ldots, n\}$.*

Remarks on the proof: It is enough to prove that there are finitely many lines D in $\mathbf{P}^2_{\mathbf{F}}$ not satisfying the above properties. In characteristic zero, this follows easily from the duality theory of plane curves. In our case, the proposition is only true under some assumptions on the characteristic, which are stated in the main theorem. □

Let $U \subset \mathbf{P}^2_{\mathbf{F}_q}$ be given by Proposition 3.1 and $s_0 \in \mathbf{N}$ be large enough so that $U(\mathbf{F}_{q^s}) \neq \varnothing$ for all $s \geq s_0$. Let $s \in \mathbf{N}$ be a sufficiently large integer; for the time being, this means that $s \geq s_0$, but another condition on s will be introduced later. For the sake of clarity, we will henceforth denote the field $\mathbf{F}_{q^s}$ by k. Fix $M \in U(k)$ and denote by $\varphi_i \colon (C_i)_k \to \mathbf{P}^1_k$ the k-morphism obtained by composing the inclusion $(C_i)_k \subset \mathbf{P}^2_k \backslash \{M\}$ with the morphism $\mathbf{P}^2_k \backslash \{M\} \to \mathbf{P}^1_k$ defined by projection from M. The morphism φ_i is finite of degree $\deg(f_i)$ and is generic, since $M \in U$. Being generic, it is separable (note that the hypotheses of Theorem 1.1 imply that $p \neq 2$); therefore there exists a smooth, complete, connected curve C_i' over k and a finite morphism $C_i' \to (C_i)_k$, such that the induced field extension $\kappa(C_i')/\kappa(\mathbf{P}^1_k)$ is a Galois closure of $\kappa((C_i)_k)/\kappa(\mathbf{P}^1_k)$. Let us write, for simplicity, $K = \kappa(\mathbf{P}^1_k)$, $K_i = \kappa(C_i')$, $G_i = \mathrm{Gal}(K_i/K)$ and $H_i = \mathrm{Gal}(K_i/\kappa((C_i)_k))$. Proposition 2.2 now shows that for all $i \in \{1, \ldots, n\}$, the curve C_i' is geometrically connected over k, the group G_i is canonically isomorphic to $\mathfrak{S}(H_i \backslash G_i)$ and the ramification indices of K_i/K are at most 2.

Let L denote the ring $K_1 \otimes_K \cdots \otimes_K K_n$. The following result, whose proof we omit, is necessary for dealing with several polynomials f_i rather than only one.

Proposition 3.2. *The ring L is a field, and k is separably closed in L.*

Let C' denote a smooth complete connected curve over k with function field L. There is a natural finite morphism $\psi \colon C' \to \mathbf{P}^1_k$, which is generically Galois and therefore separable. We denote by g the genus of C', by G the group $\mathrm{Gal}(L/K)$, by N the degree of ψ, and by $(x, L/K)$ the Artin symbol of the extension L/K above a closed point $x \in \mathbf{P}^1_k$ which does not ramify in L. We would now like to find a rational point of $\mathbf{P}^1_k$ above which the fibre of ψ is integral and use

Theorem 3.3. *(Čebotarev density theorem,* [4, Proposition 13.4]*) Let c be a conjugacy class in G. We denote by $P(L/K, c)$ the set of rational points $x \in \mathbf{P}^1(k)$ outside the branch locus of $C' \to \mathbf{P}^1_k$ such that $c = (x, L/K)$. Then one has*

$$|P(L/K,c)| \geq \frac{1}{N}\left(q^s - (N+2g)q^{s/2} - Nq^{s/4} - 2(g+N)\right). \tag{1}$$

From Theorem 3.3, we want to deduce that $P(L/K, c)$ is non-empty as soon as s is chosen large enough. Some calculations using Hurwitz's theorem [5, IV.2.4] show that g is independent of M and s, which is sufficient for what we need.

We can therefore assume that the right-hand side of (1) is at least 2, by demanding that s be sufficiently large. The canonical isomorphism $G = G_1 \times \cdots \times G_n = \mathfrak{S}(H_1\backslash G_1) \times \cdots \times \mathfrak{S}(H_n\backslash G_n)$ allows us to choose an element $\sigma \in G$ whose projection in G_i acts transitively on $H_i\backslash G_i$ for every $i \in \{1, \ldots, n\}$. Let $x_0 \in \mathbf{P}^1(k)$ be the point corresponding to the line in $\mathbf{P}^2_k$ passing through M and M_0. Theorem 3.3 now ensures the existence of a rational point $x \in \mathbf{P}^1(k)$ outside $\bigcup_{i=1}^n R_i$, distinct from x_0, and such that $\sigma = (x, L/K)$. As the image of $(x, L/K)$ in G_i is $(x, K_i/K)$, it follows from Lemma 4.1 and the definition of σ that $\varphi_i^{-1}(x)$ is irreducible. Moreover, the k-scheme $\varphi_i^{-1}(x)$ is étale since $x \notin R_i$, and hence it is integral. That $x \neq x_0$ implies that there exist $a, b \in k$ such that for every $i \in \{1, \ldots, n\}$, the scheme $\mathrm{Spec}(k[t]/(f_i(at+b, t)))$ is an open subscheme of $\varphi_i^{-1}(x)$; as the latter scheme is integral, the polynomials $f_1(at+b, t), \ldots, f_n(at+b, t)$ must be irreducible. □

4. Appendix

The following lemma is used several times in the proof of Theorem 1.1. It is essentially well-known, but we state it here and include a sketch of proof for lack of an adequate reference. It is only for technical reasons that we state it in such generality (we need to allow X' to be non-connected in order to be able to reduce to the case of a strictly Henselian base in the proof below).

Lemma 4.1. *Let $u\colon X' \to X$ and $f\colon X \to B$ denote surjective finite flat morphisms of normal schemes. Assume B is the spectrum of a discrete valuation ring. Put $f' = f \circ u$. Let G be a finite subgroup of $\mathrm{Aut}_B(X')$ such that the generic fibre of f' is a torsor under G. Let $m \in X'$ belong to the special fibre of f'. We denote respectively by $D_m \subseteq G$ and $I_m \subseteq G$ the decomposition and inertia subgroups associated with m; in other words, D_m is the stabilizer of m and I_m is the kernel of the natural map $D_m \to \mathrm{Aut}(\kappa(m))$. Let $H = G \cap \mathrm{Aut}_X(X')$. Then the double quotient $H\backslash G/D_m$ is canonically in bijection with the special fibre of f, and the double quotient $H\backslash G/I_m$ is canonically in bijection with the geometric special fibre of f.*

Sketch of proof. Let us first consider the assertion about $H\backslash G/I_m$. To prove it, one easily checks that B may be assumed to be strictly Henselian, by using the fact that for any finite field extension L/k, the group $\mathrm{Aut}_k(L)$ acts freely on $\mathrm{Spec}(L \otimes_k \bar{k})$, where $\bar{k}$ denotes a separable closure of k. Now the assertion about $H\backslash G/I_m$ follows from that about $H\backslash G/D_m$ since $D_m = I_m$.

We are thus left with the first part of the lemma. Define a map

$$H\backslash G/D_m \longrightarrow f^{-1}(f'(m))$$

by sending the double class $H\sigma D_m$ to $u(\sigma(m))$. The key ingredient for checking that this map is indeed a bijection is the transitivity of the action of G (resp. H) on the fibres of f' (resp. u), and it is a consequence of [2, Ch. 5, 2, Th. 2]. □

References

[1] A. O. Bender, O. Wittenberg, A potential analogue of Schinzel's hypothesis for polynomials with coefficients in $\mathbf{F}_q[t]$, *Internat. Math. Res. Notices* ***36*** *(2005) 2237–2248.*

[2] N. Bourbaki, Éléments de mathématique. Fasc. XXX. Algèbre commutative. Chapitre 5: Entiers. Chapitre 6: Valuations. *Actualités Scientifiques et Industrielles, No. 1308, Hermann, Paris, 1964.*

[3] K. Conrad, Irreducible Values of Polynomials: A Non-Analogy, in *Number Fields and Function Fields – Two Parallel Worlds, [G. van der Geer, B. Moonen, René Schoof, eds.] Progress in Mathematics* ***239****, Birkhäuser, Boston, MA, 2005.*

[4] W-D. Geyer, M. Jarden, Bounded realization of l-groups over global fields, *Nagoya Math. J.* ***150*** *(1998) 13–62.*

[5] R. Hartshorne, Algebraic Geometry, *Graduate Texts in Mathematics* ***52****, Springer-Verlag, New York, NY, 1977.*

[6] A. Schinzel, W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arithmetica* ***IV*** *(1958) 185–208; corrigé ibid.* ***V*** *(1958) 259.*

[7] J-P. Serre, Topics in Galois theory, *Research Notes in Mathematics* ***1****, Jones and Bartlett Publishers, Boston, MA, 1992.*

Korea Institute for Advanced Study Seoul 130-722 Korea
E-mail address: andreas@kias.re.kr