A possible generalization of Artin's conjecture for primitive root

Ching-Li Chai

February 13, 2004

§1. Artin's original conjecture

(1.1) Conjecture (Artin, 1927) *Let a be an integer, $a \neq 0, \pm 1$, and a is not a square. Let S_a be the subset of prime numbers consisting of all prime numbers p such that the image $\bar{a}$ of a in $\mathbb{F}_p$ is a generator of $\mathbb{F}_p^\times$. Then S_a is infinite.*

The following is a refinement of Artin's conjecture.

(1.2) Conjecture *Notation as in 1.1. Then S_a has positive Dirichlet density, i.e. the limit*

$$d(S_a) := \lim_{s \to 1^+} \frac{\sum_{p \in S_a} p^{-s}}{\sum_p p^{-s}} = \lim_{s \to 1^+} \frac{\sum_{p \in S_a} p^{-s}}{\log \zeta(s)}$$

exists and is a positive real number. The expected value of $d(S_a)$ is

$$A(a) := \lim_{J \to \infty} \sum_{I \subseteq J} \frac{-1^{|I|}}{[K_I : \mathbb{Q}]} = \sum_I \frac{-1^{|I|}}{[K_I : \mathbb{Q}]}.$$

In the above, I and J are finite sets of prime numbers, possibly empty. For each finite set I of prime numbers, K_I denotes the number field $\mathbb{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{a})_{\ell \in I}$.

(1.2.1) Remark The limit in the definition of $A(a)$ exists, and is equal to the absolutely convergent sum over all I's. Moreover, $A(a)$ can be expressed as an infinite product:

$$A(a) = \delta_a \cdot \prod_\ell \left(1 - [\mathbb{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{a}) : \mathbb{Q}]^{-1}\right),$$

where δ_a is a positive rational number given by an explicit formula. We do not reproduce the formula, except mentioning that $|\delta_a - 1|^{-1} \in \mathbb{N}$, and refer the reader to [Mur1] for a survey of Artin's conjecture.

(1.2.2) Remark Some results on Conjectures 1.1 and 1.2 are discussed in 3.4.

(1.3) Conjecture 1.2 can be reformulated as follows:

> There exists a subset of prime numbers p with positive density such that the specialization modulo p of the cyclic subgroup $a^{\mathbb{Z}} \subset \mathbb{G}_m(\mathbb{Q})$ is equal to $\mathbb{G}_m(\mathbb{F}_p)$.

We would like to generalize this statement to the setting of a commutative algebraic groups G over a global field K, and an arbitrary finitely generated subgroups Γ of the group of rational points $G(K)$. However we cannot simply change $\mathbb{G}_m$ to G and substitute $a^{\mathbb{Z}}$ by Γ, since the plausibility of 1.2 depends on the fact that $\mathbb{F}_p^\times$ is a cyclic group. For instance, if Γ is a cyclic subgroup of $(\mathbb{G}_m \times \mathbb{G}_m)(\mathbb{Q})$, then the specialization of Γ at any prime p is a cyclic group, hence cannot possibly be equal to $(\mathbb{G}_m \times \mathbb{G}_m)(\mathbb{F}_p) = \mathbb{F}_p^\times \times \mathbb{F}_p^\times$, because the latter is not a cyclic group.

Our idea is that, given a commutative algebraic group G over a global field K and a finitely generated subgroup $\Gamma \subset G(K)$, there should be a positive proportion of finite places v of K such that the specialization of Γ at v is "as large as possible". To make sense of the last sentence we will make a list of constraints on the specialization homomorphism s_v and the subgroup $s_v(\Gamma)$ of $\underline{G}(\kappa_v)$. Then "as large as possible" would mean "as large as allowed by those constraints".

(1.4) We assume that G is a semi-abelian variety, partly because the question is easy for unipotent commutative algebraic groups. Let $\underline{G}^{\mathrm{lft\,NR}}$ be the Néron model of G over $\mathcal{O}_K$, which is a smooth group scheme locally of finite type over $\mathcal{O}_K$ satisfying the standard universal property. Let $\underline{G}$ be the connected Néron model of G over $\mathcal{O}_K$, a smooth group scheme of finite type over $\mathcal{O}_K$, defined as the open subgroup scheme of $\underline{G}^{\mathrm{lft\,NR}}$ such that the fiber of $\underline{G}$ over each point s of $\operatorname{Spec}\mathcal{O}_K$ is the neutral component of the fiber of $\underline{G}^{\mathrm{lft\,NR}}$ over s.

(1.4.1) Let Γ be a finitely generated subgroup of $G(K)$ as above. Let Δ be the subgroup of $G(K)$ consisting of all element $t \in G(K)$ with the property that there exists a non-zero integer n such that $[n](t) \in \Gamma$, where $[n]$ is the endomorphism "multiplication by n" of G. The assumption that G is semi-abelian implies that Δ is finitely generated, and contains Γ as a subgroup of finite index. Clearly Δ contains $G(K)_{\mathrm{tor}}$, the torsion subgroup of $G(K)$, hence $\Delta_{\mathrm{tor}} = G(K)_{\mathrm{tor}}$.

(1.4.2) For each finite place v of K, denote by κ_v the residue field of $\mathcal{O}_K$ at v, and let p_v be the characteristic of the residue field κ_v of v. Denote by $\Delta_{\mathrm{tor}}^{(p_v)}$ the maximal subgroup of Δ_{tor} without p_v-torsion.

(1.4.3) Let $\Sigma_{K,f}$ be the set of all finite places v of K such that for every element $\gamma \in \Delta$, the image of $\gamma \in G(K) = \underline{G}^{\mathrm{lft\,NR}}(\mathcal{O}_K)$ in $\underline{G}^{\mathrm{lft\,NR}}(\kappa_v)$ belongs to $\underline{G}(\kappa_v)$. Notice that $\Sigma_{K,f}$ contains all but a finite number of places of K. For $v \in \Sigma_{K,f}$, denote by

$$s_v : \Gamma \to \underline{G}(\kappa_v)$$

the natural specialization map from Γ to $\underline{G}(\kappa_v)$.

(1.4.4) The following is a list of constraints on s_v and $s_v(\Gamma)$, the specialization of Γ at v.

(i) (obvious) Let H be the Zariski closure of Γ in G. Denote by $\underline{H}$ the Zariski closure of H in $\underline{G}$; $\underline{H}$ is a model of H over $\mathcal{O}_K$. Clearly, $s_v(\Gamma)$ is contained in the subgroup $\underline{H}(\kappa_v)$ of $\underline{G}(\kappa_v)$ for every $v \in \Sigma_{K,f}$.

(ii) (from group theory) The specialization map

$$s_v \, : \, \Gamma \longrightarrow \underline{G}(\kappa_v)$$

is the restriction to Γ of a homomorphism from Δ to $\underline{G}(\kappa_v)$, for every $v \in \Sigma_{K,f}$

(iii) (from algebraic geometry) For each $v \in \Sigma_{K,f}$ the restriction

$$s_v|_{\Delta_{\mathrm{tor}}^{(p_v)}} \, : \, \Delta_{\mathrm{tor}}^{(p_v)} \longrightarrow \underline{G}(\kappa_v)$$

of s_v to the prime-to-p_v torsion subgroup $\Delta_{\mathrm{tor}}^{(p_v)}$ of Δ, is injective.

The proofs are left as exercises. In the next section, we will define an algebraic notion of *maximal* (Γ, Δ)*-subgroups* to formalize the idea of being "as large as allowed by the above constraints".

§2. Maximal admissible image subgroups

(2.1) Definition Let G, Δ be abelian groups, and let Γ be a subgroup of Δ. Let Δ_{tor} be the maximal torsion subgroup of Δ, and let δ be a subgroup of the torsion subgroup $\Delta_{\mathrm{tor}} \subset \Delta$.

(i) A (Γ, Δ)-subgroup of G is a subgroup of G of the form $h(\Gamma)$, where h is a group homomorphism from Δ to G.

(ii) A homomorphism $h : \Delta \to G$ is δ*-admissible* if the restriction of h to δ is injective.

(iii) A δ*-admissible* (Γ, Δ)*-subgroup* of G is a subgroup of the form $h(\Gamma)$, for some δ-admissible homomorphism $h : \Delta \to G$.

(iv) A maximal member in the family of δ-admissible (Γ, Δ)-subgroup is called a *maximal* δ*-admissible* (Γ, Δ)*-subgroup* of G.

(iv)$'$ Suppose that G is a finite abelian group. A member in the family of δ-admissible (Γ, Δ)-subgroup with maximal cardinality is called a *strongly maximal* δ*-admissible* (Γ, Δ)*-subgroup* of G.

(v) Let R be the localization of $\mathbb{Z}$ with respect to a multiplicatively closed set of non-zero integers. An *R-maximal* δ-admissible (Γ, Δ)-*subgroup* H_0 of G is a δ-admissible (Γ, Δ)-subgroup such that $H_0 \otimes_{\mathbb{Z}} R$ is a maximal member in the family of subgroups of $G \otimes_{\mathbb{Z}} R$ of the form $H \otimes_{\mathbb{Z}} R$, where H runs through all δ-admissible (Γ, Δ)-subgroups of G.

(v)$'$ Notation as in (iv) above, and assume that G is a finite abelian group. A strongly *R-maximal* δ-admissible (Γ, Δ)-*subgroup* H_0 of G is a δ-admissible (Γ, Δ)-subgroup such that $H_0 \otimes_{\mathbb{Z}} R$ is a member with maximal cardinality in the family of subgroups of $G \otimes_{\mathbb{Z}} R$ of the form $H \otimes_{\mathbb{Z}} R$, where H runs through all δ-admissible (Γ, Δ)-subgroups of G.

(2.1.1) Terminology.

(1) A δ-admissible (Γ, Γ)-subgroup is also called a δ-admissible Γ-subgroup. A maximal δ-admissible Γ-subgroup is a maximal δ-admissible (Γ, Γ)-subgroup.

(2) Let p be a prime number, and let $\Delta_{\rm tor}^{(p)}$ be the maximal subgroup of $\Delta_{\rm tor}$ on which $[p]$ is invertible. In Def. 2.1 with $\delta = \Delta_{\rm tor}^{(p)}$, we often say "$p$-admissible" instead of "$\Delta_{\rm tor}^{(p)}$-admissible".

(3) When the group G is the group of $\mathbb{F}_q$-rational points of a commutative algebraic group over a finite field $\mathbb{F}_q$ and q is a power of a prime number p, we often simplify "p-admissible" further, to "admissible".

(4) In (v) and (v)$'$ of 2.1, when $R = \mathbb{Z}_{(\ell)}$, we often say "ℓ-maximal", or "maximal at ℓ", instead of "$\mathbb{Z}_{(\ell)}$-maximal"

(2.1.2) Examples.

- If $\Gamma \cong \mathbb{Z}$, then a maximal Γ-subgroup in G is a maximal cyclic subgroup of G. Notice that the "δ-admissible" part is superfluous here, because $\Delta = \Gamma$ has no torsion.
- If $\Gamma \cong \mathbb{Z}^r$, $r \in \mathbb{N}$, then a maximal Γ-subgroup is a subgroup of G maximal among subgroups which can be generated by r elements.
- Suppose that $\Gamma = \mathbb{Z}$, $G = (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/\ell^2\mathbb{Z})$, where ℓ is a prime number. Then every strongly maximal Γ-subgroups of G is isomorphic to $\mathbb{Z}/\ell^2\mathbb{Z}$, and is generated by an element of the form $(\bar{a}, \bar{1})$. There are maximal Γ-subgroups of G which are not strongly maximal; they are generated by an element of the form $(\bar{1}, \bar{b})$. In fact the only non-trivial subgroup of G which is not Γ-maximal is $\ell \cdot G$.

(2.2) From now on, we assume that Γ and Δ are finitely generated abelian group, and G is a finite abelian group. Let δ be a subgroup of $\Delta_{\rm tor}$, necessarily finite. For each prime number ℓ, let $G[\ell^\infty]$ be the maximal ℓ-primary torsion subgroup of G, so that G is the direct sum of the $G[\ell^\infty]$'s. For any subgroup H of G, the maximal ℓ-primary subgroup $H[\ell^\infty]$ of H is equal to $H \cap G[\ell^\infty]$, and also equal to $\mathrm{pr}_\ell(H)$, where $\mathrm{pr}_\ell : G \to G[\ell^\infty]$ denotes the natural projection. Similary, denote by $\delta[\ell^\infty]$ the maximal ℓ-primary subgroup of δ.

(2.2.1) Lemma *Notation as above. Then a δ-admissible (Γ, Δ)-subgroup H of G is a maximal δ-admissible (Γ, Δ)-subgroup if and only if the ℓ-primary subgroup $H[\ell^\infty]$ is a maximal $\delta[\ell^\infty]$-admissible (Γ, Δ)-subgroup of $G[\ell^\infty]$ for every prime number ℓ.*

Proof. Let $n \neq 0$ be a non-zero integer such that n kills G, $\Delta_{\rm tor}$ and Δ/Γ. Then the natural map $\Gamma/n\Gamma \to \Delta/n\Delta$ is an injection. The composition $\delta \hookrightarrow \Delta \to \Delta/n\Delta$ is also an injection, hence δ can be naturally identified with a subgroup of $\Delta/n\Delta$. Then every homomorphism $h : \Gamma \to G$ factors through $\Delta \twoheadrightarrow \Delta/n\Delta = \prod_\ell((\Delta/n\Delta)[\ell^\infty])$. So we obtain a natural bijection, from the set $S_{(\Gamma,\Delta),G}$ of all δ-admissible (Γ, Δ)-subgroups of G, to the product $\prod_{\ell|n} S_{(\Gamma,\Delta,n,\ell),G[\ell^\infty]}$, where $S_{(\Gamma,\Delta,n,\ell),G[\ell^\infty]}$ is the set of all $\delta[\ell^\infty]$-admissible $((\Gamma/n\Gamma)[\ell^\infty], (\Delta/n\Delta)[\ell^\infty])$-subgroups of $G[\ell^\infty]$. Notice that every $\delta[\ell^\infty]$-admissible (Γ, Δ)-subgroup of $G[\ell^\infty]$ is a $\delta[\ell^\infty]$-admissible $((\Gamma/n\Gamma)[\ell^\infty], (\Delta/n\Delta)[\ell^\infty])$-subgroup of $G[\ell^\infty]$, and vice versa. The Lemma follows. ∎

(2.2.2) Lemma *Assume that Γ is a free abelian group of finite rank, and G is a finite abelian group as before. Let $\alpha : \Gamma \twoheadrightarrow H$ be an epimorphism from Γ to a subgroup H of G. Let ℓ be a prime number. Then H is an ℓ-maximal Γ-subgroup of G if and only if the following conditions are satisfied.*

(i) *The natural homomorphism $H/\ell H \to G/\ell G$ is injective.*

(ii) $\dim_{\mathbb{F}_\ell}(\mathrm{Ker}(\Gamma/\ell\Gamma \to H/\ell H)) = \mathrm{Max}\,(0, \dim_{\mathbb{F}_\ell}(\Gamma/\ell\Gamma) - \dim_{\mathbb{F}_\ell}(G/\ell G))$. *In other words, if $H/\ell H \neq G/\ell G$, then α induces an isomorphism from $\Gamma/\ell\Gamma$ to $H/\ell H$. Another way to say the same thing is that the map $\alpha \otimes (\mathbb{Z}/\ell\mathbb{Z}) : \Gamma/\ell\Gamma \to G/\ell G$ is either an surjection or an injection.*

§3. A general version of Artin's conjecture

(3.1) Let G be a semi-abelian variety over a global field K, and let Γ be a finitely generated subgroup of $G(K)$ such that Γ is Zariski dense in G. We follow the notation as in 1.4, and introduce some more below.

(3.1.1) For each finite set I of prime numbers, let $M_{\Gamma,I}$ be the subset of $\Sigma_{K,f}$, consisting of all elements $v \in \Sigma_{K,f}$ such that $s_v(\Gamma)$ is an ℓ-maximal p_v-admissible (Γ, Δ)-subgroup of $\underline{G}(\kappa)$ for every $\ell \in I$.

(3.1.2) Let J be a finite set of prime numbers. Denote by $S_\Gamma^{(J)}$ the subset of $\Sigma_{K,f}$ consisting of all elements $v \in \Sigma_{K,f}$ such that $s_v(\Gamma)$ is an ℓ-maximal p_v-admissible (Γ, Δ)-subgroup of $\underline{G}(\kappa)$ for every $\ell \notin J$.

(3.2) Conjecture *Notation as above.*

(i) *For every subset I of prime numbers, the subset $M_{\Gamma,I}$ of $\Sigma_{\Gamma,f}$ has a Dirichlet density,, i.e. the limit*

$$d_I := \lim_{s\to 1^+} \frac{\sum_{v\in M_{\Gamma,I}} \mathrm{N}_v^{-s}}{\log \zeta_K(s)}$$

exists. Note that $d_I \geq d_{I'}$ if $I \subseteq I'$.

(ii) *Let J be a finite set of prime numbers. Then the subset $S_\Gamma^{(J)}$ has a Dirichlet density, i.e.*

$$d(S_\Gamma^{(J)}) := \lim_{s\to 1^+} \frac{\sum_{v\in S_\Gamma^{(J)}} \mathrm{N}_v^{-s}}{\log \zeta_K(s)}$$

exists, and is equal to the decreasing limit

$$\lim_{\substack{I\to\infty \\ I\cap J=\emptyset}} d_I\,,$$

where I runs through all finite sets I of prime numbers such that $I \cap J = \emptyset$.

(iii) *The density of $S_\Gamma^{(J)}$ is equal to zero if and only if there exists a finite set I of prime numbers such that $I \cap J = \emptyset$ and $d_I = 0$.*

The following is a conjecture on the positivity of $d(S_\Gamma^{(J)})$, supplementing 3.2 (iii).

(3.2.1) Conjecture *There exists a finite set of prime numbers J_0 such that $d(S_\Gamma^{(J_0)}) > 0$*

Remark In the case when $G = \mathbb{G}_m$, $K = \mathbb{Q}$, and Γ is the cyclic group generated by an element $a \in K^\times$, The conjunction of Conjectures 3.2 and 3.2.1 reduce to Conjecture 1.2.

(3.3) We mention two variants of Conjecture 3.2. First, instead of using p_v-admissible (Γ, Δ)-subgroups which are maximal at all $\ell \notin J$, we can consider the subset $Z_\Gamma^{(J)}$ of all places $v \in \Sigma_{K,f}$ such that the p_v-admissible subgroup $s_v(\Gamma) \subseteq \underline{G}(\kappa_v)$ is strongly maximal at all primes $\ell \notin J$.

The second variant is to impose a generalized congruence relation: Let E be a finite Galois extension of K, and let $C \subset \mathrm{Gal}(E/K)$ be a union of conjugacy classes in $\mathrm{Gal}(E/K)$. Let $M_{\Gamma,C}^{(J)}$ be the set consisting of all $v \in \Sigma_{K,f}$ such that $\mathrm{Fr}_v \subseteq C$ and the p_v-admissible subgroup $s_v(\Gamma) \subseteq \underline{G}(\kappa_v)$ is maximal at all primes $\ell \notin J$. Then we have an obvious analogue of Conjecture 3.2. Note that the condition $\mathrm{Fr}_v \subseteq C$ is slightly ambiguous if v is ramified in E. However this ambiguity has no effect on the conjecture, as only a finite number of places are involved.

(3.4) Conjectures 3.2 and 3.2.1 have been proved in the following cases.

- Bilharz 1937: $G = \mathbb{G}_m$, $\Gamma \cong \mathbb{Z}$, and K is a global function field.
- Hooley, 1967: $G = \mathbb{G}_m$, $\Gamma \cong \mathbb{Z}$, $K = \mathbb{Q}$, and assumes the generalized Riemann hypothesis.
- Lenstra, 1977: $G = \mathbb{G}_m$, Γ arbitrary, assuming GRH in the number fields case. The main innovation is the positivity statement (iii) of Conj. 3.2.
- Chen, Kitaoka and Yu, 2003: K is a global function field, $\Gamma \cong \mathbb{Z}$, and G is a one-dimensional torus over K.

Gupta and Murty exhibited many finite sets S of integers such that there such that Conjecture 1.1 holds for at least one element $a \in S$. In their original paper [GM1], the set S has 13 elements. Later the cardinality of S was lowered to 3, with $\{2, 3, 5\}$ as an example; see [Hea].

§4. Comments

(4.1) The standard strategy for proving Artin's conjecture is as follows. First, one constructs a family of finite Galois extensions L_ℓ/K and a subset $Z_\ell \subseteq \mathrm{Gal}(L_\ell/K)$ stable under conjugation, such that $s_v(\Gamma)$ is *not* maximal at ℓ if and only if the Frobenius conjugacy class $\mathrm{Fr}_{v,L_\ell/K} \subseteq Z_\ell$. (We ignore the slight ambiguity when v is ramified in L_ℓ/K.) Usually L_ℓ/K and Z_ℓ are constructed from some homomorphism from $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ to a finite group. Such an algebraic construction would settle the easier part (i) of Conj. 3.2, in view of the Chebotarev density theorem. According to Lemma 2.2.1, an element $v \in \Sigma_{K,f}$ is in $S^{(J)}_{\Gamma,\Delta}$ if and only if $\mathrm{Fr}v, L_\ell/K \not\subseteq Z_\ell$ for all primes $\ell \notin J$. This brings us to a standard sort of sieve problem, familiar in works on Artin's original conjecture.

(4.2) For a torus over a global function field, Conjectures 3.2 and 3.2.1 may be within reach with available technology. The situation is similar for a torus over a number field, if one assumes the GRH. For abelian varieties over a global function field, the question becomes more interesting, because the ℓ-adic representation attached to an abelian variety is more complicated than the case of tori; in the latter case the image of the ℓ-adic representation is finite. In another direction, one would also want to investigate the obvious generalizations of 3.2 and 3.2.1 for a torus over the function field of a variety over a finite field.

References

[Bi] H. Bilharz. Primdivisoren mit vorgegebener Primitivwurzel. *Math. Ann.*, 114:476–492, 1937.

[CKY] Y. M. Chen, Y. K. Kitaoka and J. Yu. On primitive roots of tori: The case of function fields. *Math. Z.*, 243:201–215, 2003.

[CK] D. A. Clark and M. Kuwata. Generalized Artin's conjecture for primitive roots and cyclicity mod $\wp$ of elliptic curves over function fields. *Canadian Math. Bulletin*, 38:167–173, 1995.

[GM1] R. Gupta and M. R. Murty. A remark on Artin's conjecture. *Inv. Math.*, 78:127–130, 1984.

[GM2] R. Gupta and M. R. Murty. Primitive points on elliptic curves. *Comp. Math.*, 58:13–44, 1986.

[Hea] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math.*, 37:27–38, 1986.

[Hei] H. A. Heilbronn. On an inequality in the elementary theory of number. *Proc. Cam. Phil. Soc.*, 33:207–209, 1937.

[Ho1] C. Hooley. On Artin's conjecure. *J. reine angew. Math.*, 225:209–220, 1967.

[Ho2] C. Hooley. *Application of Sieve Methods to the Theory of Numbers.* Cambridge Tracts in Math, **70**, Cambridge Univ. Press, 1976.

[Le] H. W. Lenstra Jr. On Artin's conjecture and Euclid's algorithm in global fields. *Inv. Math.*, 42:201–224, 1977.

[Mur1] M. R. Murty. Artin's conjecture for primitive roots. *Math. Intelligencer*, 10:59–67, 1988.

[MS] M. R. Murty and S. Srinivasan. Some remarks on Artin's conjecture. *Canadian Math. Bulletin*, 30:80–85.

[Vi] A. I. Vinogradov. Artin L-series and his conjectures. *Proc. Steklov Inst. Math.*, 112:124-142, 1971.