Algebraic groups and discrete logarithm

J.-M. Couveignes*

Abstract

We prove two theorems and raise a few questions concerning discrete logarithms and algebraic groups.

1 Introduction

Je n'aurais jamais pensé que mes pièces dussent s'attirer l'immortalité; mais depuis que quelques poètes fameux m'ont fait l'honneur de les parodier, ce choix de préférences pourrait bien, dans les temps à venir, leur faire partager une réputation qu'elles ne devront originairement qu'aux charmantes parodies qu'elles auront inspirées. Aussi marquai-je d'avance à mes associés bénévoles, dans ce nouveau livre, toute la reconnaissance que m'inspire une société aussi flatteuse, en leur fournissant, dans ce troisième ouvrage, un vaste champ pour exercer leur Minerve.
François Couperin, *Préface au troisième livre*

This paper, based on two talks given in Bordeaux (*Three days in computational analytic and elementary number theory*, may 1998) and Durham (*Computational number theory*, july 2000) is devoted to the study of discrete logarithm in a slightly more general context than usual.

In section 3 we give the weakest conditions we know for the existence of a *proven* sub-exponential algorithm computing discrete logarithms in the jacobians of curves with increasing genera over a fixed field. The first work in that context is [2] and was repeated in a series of publications all assuming more less implicitly the curves to have very special geometric properties (e.g. being super-elliptic). We show this is an inessential property. We replace it by a more arithmetic one concerning the asymptotic behavior of the size of the jacobian. We believe it has not been stressed enough that the genus does not suffice to control this size (e.g. up to a sub-exponential factor). So it is not reasonable to expect discrete logarithm algorithms to exist that would not take this problem into account. I would like to thank Christophe Betard with whom I had many interesting discussions on that topic. The algorithm we give relies on no heuristic and therefore gives a theorem on the (randomized) complexity of discrete logarithms in the Picard group of curves over a fixed field.

*Groupe de Recherche en Informatique et Mathématiques du Mirail, Université de Toulouse II, Le Mirail

Conversely, in section 4 we define the category of easy algebraic groups and study the problem of discrete logarithm in the groups of points of a fixed algebraic group, rational over increasing finite fields. We show that this category has quite nice properties.

This leads to very natural questions of algorithmic and geometric nature.

Section 2 sets or recalls a few natural and simple definitions from complexity theory to ensure the accuracy of the statements in that work.

2 Discrete logarithm problems and their complexity

Since we shall be concerned with the difficulty of computing discrete logarithms we first give the next

Definition 1 *A discrete logarithm problem $(\mathcal{G}, \alpha, \beta)$ consists of a finite computational commutative group $\mathcal{G}$, an element α in $\mathcal{G}$, and an element β in $\mathcal{G}$. A solution to this problem consists of an integer k such that $\beta = k\alpha$.*

We do not assume the order of the group $\mathcal{G}$ to be known. We may slightly generalize the previous definition with

Definition 2 *An extended discrete logarithm problem $(\mathcal{G}, (\alpha_a)_{1\leq a\leq A}, \beta)$ consists of a finite computational commutative group $\mathcal{G}$, a family $(\alpha_a)_{1\leq a\leq A}$ of elements in $\mathcal{G}$, and an element β in $\mathcal{G}$. A solution to this problem consists of A integers $(k_a)_{1\leq a\leq A}$ such that $\beta = \sum_a k_a\alpha_a$.*

Although the extended logarithm problem seems to be more difficult than the ordinary one, we notice that all known algorithms for the second one straightfully extend to the first one.

In the sequel we shall concentrate on plain discrete logarithm problem. An algorithm for solving discrete logarithm will be a *randomized* algorithm that gives a solution when it exists but may run indefinitely when there is no solution. Such an algorithm with known complexity may be used to solve the decision problem (existence or not of a solution) in a *probabilistic* way. This means that we may bound the probability of giving a wrong (negative) answer by an arbitrary small constant.

Another use of a generalized discrete logarithm random algorithm is to compute the module of relations between elements $(\alpha_a)_{1\leq a\leq A}$ of a commutative group $\mathcal{G}$ with given cardinality I, that is the kernel $\mathcal{R}$ of the map ξ in

$$0 \to \mathcal{R} \to \mathbb{Z}^A \xrightarrow{\xi} \mathcal{G}.$$

This problem is solved, at least in a *probabilistic* way, by first factoring (with a sieving method like in [8]) the cardinality I. One then computes the order $h_{1,1}$ of α_1 which is a divisor of I. Then, one looks for the smallest divisor $h_{2,2}$ of I such that $h_{2,2}\alpha_2$ is in the subgroup $< \alpha_1 >$ generated by α_1. This is done using the generalized discrete logarithm algorithm. We find $h_{2,2}\alpha_2 + h_{2,1}\alpha_1 = 0$. We continue this way and find the Hermite normal form of $\mathcal{R}$.

An application is to compute a generating set for the intersection

$$\mathcal{H} \cap < \alpha_1, ..., \alpha_A >$$

where $\mathcal{H}$ is a subgroup of $\mathcal{G}$, provide we are given the cardinality of $\mathcal{G}/\mathcal{H}$ and a generating set for $\mathcal{H}$.

We are interested in the randomized complexity of discrete logarithms. We say that a family of discrete logarithm problems is *easy* if there exists a randomized algorithm that solves these problems in sub-exponential time in the order of the group $\mathcal{G}$ that is in time $\exp(O(1)\log^\alpha |\mathcal{G}|)$ for some α in $]0,1[$. Basic operations in the group are assumed to require polynomial time in the logarithm of the size of the group.

We say that a family of groups is *easy* if the family of all discrete logarithm problems involving any of these groups is solved in time $\exp(O(1)\log^\alpha |\mathcal{G}|)$ for some α in $]0,1[$.

It is a simple consequence of Kraitchik's index calculus method that the family of all multiplicative groups of prime finite fields is easy (we can take any $\alpha > 1/2$). Similarly, the family of all multiplicative groups of finite fields of given characteristic is easy.

It is shown in [1] that the family of multiplicative groups of all finite fields is easy under some reasonable though unproven conjectures.

3 Index calculus and Picard groups

In this section we prove the following

Theorem 1 *Let $(\mathcal{C}_i)_{i\geq 1}$ be a family of curves over $\mathbb{F}_q$ with genus $\gamma_i = g(\mathcal{C}_i)$ tending to infinity and assume the number $\#\mathcal{J}_{\mathcal{C}_i}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on the jacobian of $\mathcal{C}_i$ is bounded by $q^{\gamma_i + O(\sqrt{\gamma_i})}$. The curves $\mathcal{C}_i$ are given as plane curves with polynomial degree in the genus. Assume further we are given an $\mathbb{F}_q$-rational point O_i on the smooth model of $\mathcal{C}_i$ for every i. Then there exists an algorithm that computes discrete logarithms in the groups $\mathcal{H}_i = \mathcal{J}_{\mathcal{C}_i}(\mathbb{F}_q)$ in random sub-exponential time $q^{O(\gamma_i^{0.5+\epsilon})}$ for any positive ϵ.*

Section 3.1 recalls a few basic facts about the algorithmics of algebraic curves. We find it necessary since our experience is that the amazing recent development of this topic tends to hide the existence of quite old and useful results (after all, the theory of algebraic curves was very much algorithmic in its origins). The proof for theorem 1 is given in section 3.2.

3.1 Basic algorithms for algebraic curves

In this section we review a few basic facts about the algorithmics of algebraic curves. We shall represent any curve over $\mathbb{F}_q$ as a plane curve $\mathcal{C}$ with degree d and genus g and will assume that the degree is bounded polynomially in the genus. This is just intended to avoid artificial examples like a series of plane genus zero curves with degree tending to infinity. *Computing a smooth model* from the plane model is then done in polynomial time in the genus. For most purposes, it suffices to have an explicit description of the different places above any singular point. These places may be given by the Puiseux expansion of one coordinate in terms of the other.

By a divisor we always mean a divisor on the smooth model of the curve although the plane model might be more convenient for practical computation. Similarly, the Picard group and the jacobian $\mathcal{J}_\mathcal{C}$ of $\mathcal{C}$ always are the ones of the smooth model.

Computation of the linear space of a divisor $A-B$ where A and B are effective divisors is then done in time polynomial in the product $\deg(A) \times \deg(B) \times g$.

The *enumeration of all prime divisors* of degree bounded by a constant c is done in polynomial time in $q^c \times g$.

Elements in the Picard group of degree 0 are represented by divisors of degree zero and computation with such divisors relies on *reducing divisors* that is finding an equivalent divisor of the form $A - gO$ with A effective which can be done in polynomial time. Here, a rational origin O is assumed to exist and to be given.

The techniques described above are very classical. See [5] for a classical review of this folklore and [9] for an updated survey taking into account the progress of computer algebra.

We now come to the problem of *choosing a random element in the Picard group* of $\mathcal{C}$ over $\mathbb{F}_q$. We do not assume the size of this group to be known. We just assume we are given a set $\mathcal{B}$ of divisor classes that generate the Picard group. We assume that the size of $\mathcal{B}$ is polynomial in the genus. Let $\Upsilon > 1$ be a real number. We want to choose a random combination of elements in $\mathcal{B}$ in such a way that the corresponding sum in the Picard group is random with Υ-*almost uniform probability*. This means that every element occurs with probability at least Υ^{-1} and at most Υ times the inverse of the size of the Picard group $\mathcal{G}$. This is achieved in the following way. Let d be the size of $\mathcal{B}$ and I the size of the Picard group. We assume $d \geq 2$, otherwise the problem is trivial. Let $\mathcal{R}$ be the kernel of the generating map ξ

$$0 \to \mathcal{R} \to \mathbb{Z}^d \xrightarrow{\xi} \mathcal{G} \to 0$$

and set $\rho = d4^d(d!)^2 I$. From Minkowski theorems [6, II.6.8,II.6.9,II.7.4] we deduce that $\mathcal{R}$ has a fundamental parallelogram $\mathcal{P}$ of radius bounded by ρ.

Let $\epsilon = 1 - \Upsilon^{-1}$. Let R be an even integer bigger than $\epsilon^{-1}d\rho$. Let C_R be the hypercube in $\mathbb{R}^d$ with center the origin and edge R defined to be the set of points with integral coordinates in the interval $[-R/2, R/2[$. It is of course very easy to pick an element in C_R with random uniform probability. The map ξ pushes the uniform probability on C_R to a probability on the set $\mathcal{G}$ which is Υ-almost uniform thus solving the problem of choosing random elements in the Picard group in polynomial time provide we use the fast exponentiation algorithm. To prove that this probability is Υ-uniform we set $r = R - \rho$ and consider the union

$$A = \bigcup_{\substack{z \in \mathcal{R} \\ z + \mathcal{P} \cap C_r \neq \emptyset}} z + \mathcal{P}$$

of $\mathcal{R}$-translates of the fundamental parallelogram $\mathcal{P}$ that meet C_r. We easily check that $C_r \subset A \subset C_R$ and $|C_R - A|/|C_R| \leq |C_R - C_r|/|C_R| \leq d\rho/R$. We similarly set $s = R + \rho$ and

$$B = \bigcup_{\substack{z \in \mathcal{R} \\ z + \mathcal{P} \cap C_R \neq \emptyset}} z + \mathcal{P}$$

the union of $\mathcal{R}$-translates of the fundamental parallelogram $\mathcal{P}$ that meet C_R. We have $C_R \subset B \subset C_s$ and $|B - C_R|/|C_R| \leq |C_s - C_R|/|C_R| \leq d\rho/R$. The result follows. On the way, we have proven the following useful

Lemma 1 *Let $\mathcal{R}$ be a sub-lattice of $\mathbb{Z}^d$ with index I and set $\kappa_d = d^2 4^d (d!)^2$. Let R be an even integer bigger than $\kappa_d I$. Let a be an element in the quotient group $\mathbb{Z}^d/\mathcal{R}$. Then the proportion of points in C_R that are congruent to a modulo $\mathcal{R}$ is in $[(1 - \kappa_d I/R)/I, (1 + \kappa_d I/R)/I]$.*

In case $\mathcal{R}$ is a subgroup of $\mathbb{Z}^d$ of rank smaller than d we have the even simpler

Lemma 2 *Let $\mathcal{R}$ be a subgroup of $\mathbb{Z}^d$ with infinite index. Let R be an even positive integer. Let a be an element in the quotient group $\mathbb{Z}^d/\mathcal{R}$. Then the proportion of points in C_R that are congruent to a modulo $\mathcal{R}$ is bounded by $1/R$.*

Remark 1 *The considerations above apply to the more general situation of a finite commutative group given by generators (relations are unknown) and allow to pick random elements with almost uniform probability as soon as an estimate is given for the size of the group.*

3.2 Proof of theorem 1

In order to prove theorem 1 we shall first describe an algorithm and then the complexity analysis for it.

Let $\mathcal{C}_i$ be any curve in the family. We denote by I the cardinality of its Picard group over $\mathbb{F}_q$. Since it is not known, we shall replace it by a majoration of it in all the estimates bellow. A discrete logarithm problem consists of two effective divisors A and B of degree γ_i. The solution is an integer k such that $[B-\gamma_i O_i] = k[A-\gamma_i O_i]$ whenever it exists.

We denote by $\mathcal{B}_i$ the set of divisors on $\mathcal{C}_i$ of degree lower than or equal to $7\sqrt{\gamma}_i$. We denote by $\bar{\mathcal{B}}_i$ the set of divisor classes of the form $[D - \deg(D)O_i]$ where D is in $\mathcal{B}_i$. One easily checks (using Riemann hypothesis for function fields) that these divisor classes generate the full Picard group of $\mathcal{C}_i$ over $\mathbb{F}_q$. We say that a divisor is $\mathcal{B}_i$-smooth or just smooth if it is a linear combination of elements in $\mathcal{B}_i$. We denote by d the cardinality of $\mathcal{B}_i$. From [12, Corollary V.2.10] we have $d = q^{7\sqrt{\gamma}_i + O(\log \gamma_i)}$. The number of effective divisors with degree $2\gamma_i$ whose all prime divisors are in $\mathcal{B}_i$ is at least

$$\frac{d^{\lfloor \frac{2}{7}\sqrt{\gamma}_i \rfloor}}{\lfloor \frac{2}{7}\sqrt{\gamma}_i \rfloor !}.$$

Indeed, to any unordered family of $\lfloor \frac{2}{7}\sqrt{\gamma}_i \rfloor$ elements in $\mathcal{B}_i$ we associate their product and thus form the expected number of smooth effective divisors. In this expression, the numerator is $q^{2\gamma_i + O(\sqrt{\gamma}_i \log \gamma_i)}$ and the denominator is $q^{O(\sqrt{\gamma}_i \log \gamma_i)}$ so we have at least $q^{2\gamma_i + O(\sqrt{\gamma}_i \log \gamma_i)}$ effective divisors of degree $2\gamma_i$ that are $\mathcal{B}_i$-smooth.

As expected the algorithm goes in several steps.

Step 1 : We first express $\alpha = [A - \gamma_i O_i]$ and $\beta = [B - \gamma_i O_i]$ as linear combinations of elements in $\bar{\mathcal{B}}_i$. To this end, we choose a linear combination of elements in $\bar{\mathcal{B}}_i$ such that the corresponding sum in the Picard group of $\mathcal{C}_i$ over $\mathbb{F}_q$ is random with 10/9-almost uniform probability (we take random coordinates in C_R with $R = 10d\rho$ where $\rho = d4^d(d!)^2 I$.) We call $D = D^+ - \gamma_i O_i$ the corresponding reduced divisor and compute the linear space $\mathcal{L}(A + D + \gamma_i O_i)$ and pick a random function ϕ in it. We set

$$(\phi) = E - A - D^+$$

where E is an effective divisor of degree $2\gamma_i$. If E is smooth, we thus get an expression of $\alpha = [A - \gamma_i O_i]$ as a linear combination of smooth divisor classes. We repeat *the whole process* (taking another random element in the jacobian) until we have found a relation.

We do the same with β.

Step 2 : We then look for linear relations between elements in $\bar{\mathcal{B}}_i$. Again we choose a linear combination of elements in $\bar{\mathcal{B}}_i$ such that the corresponding sum in the Picard group of $\mathcal{C}_i$ over $\mathbb{F}_q$ is random with 10/9-almost uniform probability. We call $D = D^+ - \gamma_i O_i$ the corresponding reduced divisor and compute the linear space $\mathcal{L}(2\gamma_i O_i + D)$ and pick a random function ϕ in it. If $(\phi) = E - D^+ - \gamma_i O_i$ with E a $\mathcal{B}_i$-smooth effective divisor, we get a linear relation. We repeat the process until we have found d independent relations.

Step 3 : We now have a lattice $\mathcal{T} \subset \mathbb{Z}^d$ of relations and we compute its volume K which is a multiple of I bounded by $(R + 2\gamma_i)^d d^d$. We look for an integer k such that $\beta = k\alpha$ in $\mathbb{Z}^d/\mathcal{T}$. This is done by mere linear algebra. If such a k exists, we output it and stop. If such a k does not exist, we try to enlarge $\mathcal{T}$ by looking for extra linear relations. We proceed as in step 2 but this time allow coefficients in C_Q with $Q = 10d\rho'$ with $\rho' = d4^d(d!)^2K$. We go on enlarging $\mathcal{T}$ until we find some k.

Remark 2 *The above algorithm solves discrete logarithm in random sub-exponential time which means that if some k exists, it shall be found in random sub-exponential time. However, if k does not exist, the algorithm will run indefinitely. This algorithm may also be used to compute the cardinality and the structure of the Picard group in probabilistic sub-exponential time as explained in section 2.*

Remark 3 *It may look strange that we use so big coefficients in the linear combinations. This is to ensure the almost uniformity of the probability distributions. In practice, one may rely on heuristics and take smaller coefficients. The necessity of translating the divisor by a random element in the jacobian instead of looking for smooth functions in a fixed linear space is also quite theoretical. However one may suspect that heuristics concerning the density of smooth functions in a given linear space (like the ones in [2]) turn to be false for some very special infinite series of curves. By contrast we notice that our algorithm makes no use of smooth functions (just smooth divisors).*

As for the complexity analysis of step 1 of the algorithm, we observe that this first step consists in taking a random element in the set $\mathcal{S}$ with cardinality $R^d q^{\gamma_i+1}$ of pairs consisting of a point in C_R and a function in the corresponding linear space. The lucky elements in this set are made of in the following way: take a $\mathcal{B}_i$-smooth divisor E of degree $2\gamma_i$. Then to any point in C_R that is mapped onto $[E - A - \gamma_i O_i]$ by ξ there corresponds a lucky element in $\mathcal{S}$. The number of lucky elements is thus at least the number of smooth divisors of degree $2\gamma_i$ times the minimum number of elements in C_R in a given class modulo $\mathcal{R}$. We thus have at least $0.9R^d q^{2\gamma_i+O(\sqrt{\gamma}_i \log \gamma_i)}/I$ lucky elements. Since $I = q^{\gamma_i+O(\sqrt{\gamma}_i)}$, the proportion of lucky elements is $q^{O(\sqrt{\gamma}_i \log \gamma_i)}$.

For step 2 we have to remove from the subset of lucky elements, those who lead to relations that are in the sub-lattice generated by the relations we already found. But this lattice is of infinite index and from lemma 2 we loose at most $1/R$ of the lucky elements.

For step 3 we again have to remove from the subset of lucky elements, those who lead to relations that are in the sub-lattice generated by the relations we already found. This time the lattice $\mathcal{T}$ has finite index at least two in $\mathcal{R}$ but since we allow coefficients of size Q the proportion of lucky elements to remove is at most 0.5×1.1. This finishes the proof of theorem 1. $\square$

Remark 4 *If $(\mathcal{C}_i)_{i\geq 1}$ is an infinite family of curves that are all coverings of the projective line of degree bounded by a constant n, then from [3, Th. 3] the class number is $O(q^g(g\log q)^{n-1})$ thus the conditions of theorem 1 are met. This is the case in particular for super-elliptic curves.*

If one takes arbitrary curves of increasing genera γ_i there is no evidence that they form an easy family of discrete logarithm problems although their jacobians are quite computational groups as soon as we avoid fancy models. This point seems to be ignored in the literature where people tend to assume (often implicitly) the existence of a map of fixed degree to the projective line. A geometric condition which is useless and quite stronger than the arithmetic condition we assume.

4 Easy algebraic groups

> Que si l'on te reproche que tu ne parles pas le langage des villageois, et que toi ni ta troupe ne sentez guère les brebis ni les chèvres, réponds leur, ma bergère, que pour peu qu'ils aient connaissance de toi, ils sauront que tu n'es pas, ni celles aussi qui te suivent, de ces bergères nécessiteuses, qui, pour gagner leur vie, conduisent les troupeaux aux pâturages, mais que vous n'avez toutes pris cette condition que pour vivre plus doucement et sans contrainte. Que si vos conceptions et paroles étaient véritablement telles que celles des bergers ordinaires, ils auraient aussi peu de plaisir de vous écouter, que vous auriez beaucoup de honte à les redire.
> Honoré d'Urfé, *Epître-Préface de l'auteur à la bergère Astrée*

In the previous section we studied the asymptotic complexity of discrete logarithms in Picard groups of algebraic curves over a fixed field. In this section, on the contrary, we study discrete logarithms in the group of points of a fixed algebraic group over increasing extensions of the base field.

An algebraic group G over $\mathbb{F}_q$ will be given as a finite collection of disjoint regular varieties all defined over $\mathbb{F}_q$ with multiplication and inversion morphisms also defined over $\mathbb{F}_q$ (see [10].) In some cases (e.g. jacobian varieties) one may prefer to work with more natural models. The choice of a model is not decisive as far as pushing a point from one model to the other one requires a constant number of operations in the field of definition of that point.

In this paper we only consider *commutative* algebraic groups.

Definition 3 *Let p be a prime and $\mathbb{F}_q$ the field with $q = p^d$ elements. Let G be a commutative algebraic group over $\mathbb{F}_q$. We say that G is an easy algebraic group over $\mathbb{F}_q$ if there exists an algorithm that solves discrete logarithm problems in the groups $\mathcal{G}_k = G(\mathbb{F}_{q^k})$ in sub-exponential random time in the size $|\mathcal{G}_k|$ of* *the groups. An operation in the base field* $\mathbb{F}_q$ *is assumed to require one unit of time. So we say that* G *is easy if and only if there exists a real* α *in* $]0,1[$ *and a randomized algorithm that computes discrete logarithms in the groups* $\mathcal{G}_k$ *in time* $\exp(O(1)\log^\alpha|\mathcal{G}_k|)$.

We notice that an algebraic group over $\mathbb{F}_q$ is easy if an only if the family of groups $G(\mathbb{F}_{q^r})$ for $r \geq 1$ is easy.

Remark 5 *We may give a more accurate definition and specify a value for* α. *For example we may say that a group is* γ*-easy if one can take in the previous definition* $\alpha = \gamma + \epsilon$ *for any positive* ϵ. *However, all the proven sub-exponential algorithm for discrete logarithms and factoring integers correspond to the case* $\gamma = 1/2$. *See remark 6.*

We start with a few lemmata.

Lemma 3 *Let* G *be a commutative algebraic group over* $\mathbb{F}_q$*, of dimension* d. *For any positive integer* r*, the size of* $G(\mathbb{F}_{q^r})$ *is equivalent to a constant* c *times* q^{dr} *when* r *tends to infinity:*

$$|G(\mathbb{F}_{q^r})| = q^{dr}(c + o(1)).$$

The cardinality of $G(\mathbb{F}_{q^r})$ is equal to the number of connected components times the cardinality of $G_0(\mathbb{F}_{q^r})$ where G_0 is the identity component (recall G/G_0 is assumed to decompose over $\mathbb{F}_q$.) The lemma then follows from some weak form of Weil's conjectures (for a non complete variety) like in [4, Corollary 5]. □

Lemma 4 *Let* G *be a commutative connected algebraic group over a finite field and let* $1 \to L \to G \to A \to 1$ *be the strict exact sequence of connected commutative algebraic groups from Chevalley's theorem. There exists an isogeny defined over* $\mathbb{F}_q$ *from* G *to the direct product* $L \times A$.

This results from the properties of the Ext functor for algebraic groups ([11, Proposition VII.6] and [11, Théorème VII.12]), the solvability of commutative linear groups (Rosenlicht [10]) and the computations for G_a and G_m ([11, Théorème VII.6, Théorème VII.7]). □

We list natural properties of easy groups in the following

Theorem 2 *The following are true.*

i — *If* $Q = q^a$ *is a power of* q *and* $\mathbb{F}_Q \supset \mathbb{F}_q$ *the corresponding field extension and* G *an algebraic group over* $\mathbb{F}_q$ *then* G *is an easy group over* $\mathbb{F}_q$ *if and only if* $G \otimes_{\mathbb{F}_q} \mathbb{F}_Q$ *is an easy group over* $\mathbb{F}_Q$.

ii — *Algebraic groups of dimension zero are easy. A group G is easy if and only if the component of the identity G_0 is easy.*

iii — *Subgroups and direct product of easy groups are easy. An isogenous group to an easy group is easy.*

iv — *If A, B and C are algebraic groups over $\mathbb{F}_q$ with a strict exact sequence*

$$1 \to A \to B \to C \to 1$$

then B is easy if and only if A and C are.

v — *The multiplicative group G_m and the additive group G_a are easy over $\mathbb{F}_p$. Linear groups are easy. A connected algebraic group is easy if and only if its maximal complete quotient is an easy abelian variety.*

vi — *Any super-singular elliptic curve is easy over its field of definition.*

Points *i*, *ii* and *iii* are trivial.

If $1 \to A \to B \to C \to 1$ is a strict exact sequence of commutative algebraic groups and A and C are easy then B is easy since we can push a discrete logarithm problem (α, β) from B to C and find k such that $\beta\alpha^k$ is in A. Because we know the order of the group of rational points of C (from Weil's conjectures) we may factor it using a sieving method and compute the smaller positive power of α lying in A. We thus reduce to a discrete logarithm problem in A. This proves half of point *iv*.

The additive group is trivially easy and also the multiplicative group by the index calculus method. Linear commutative groups are solvable (Rosenlicht [10]) therefore easy. If $1 \to L \to G \to A \to 1$ is the exact sequence from Chevalley's theorem then A is isogenous to a subgroup of G by lemma 4 and is thus easy if G is. The converse follows from what we just proved of point *iv*. Therefore quotients of easy groups are easy. This finishes the proof of point *iv*.

Assertion *vi* is the result in [7]. $\square$

Remark 6 *The theorem above remains true if we replace everywhere the word easy by α-easy (following remark 5) provide $\alpha \geq 1/2$. This condition is imposed by the use of a proven factoring algorithm in proving point iv. One may of course wonder if there are provable factoring algorithms for a smaller α (see related question 4 below).*

We denote by AG_q the category of algebraic groups over $\mathbb{F}_q$ and AG_0 the category of algebraic groups over $\bar{\mathbb{F}}_q$. We denote by EAG_q the full sub-category of AG_q consisting of easy algebraic groups over $\mathbb{F}_q$ and similarly for EAG_0.

We ask how large are EAG_q and EAG_0. In view of Chevalley's theorem [10] and theorem 2 we may restrict our attention to simple abelian varieties over $\bar{\mathbb{F}}_q$.

It is remarkable that there has been no result in the sense of enlarging these categories since the proof by Menezes, Okamoto and Vanstone [7] of statement *vi* in theorem 2.

From the properties listed above we can expect the category EAG_0 to be characterized by simple geometric ways. This raises the following

Question 1 *How big is* EAG_0*?*

More accurate questions

Question 2 *Are all abelian varieties easy?*

Question 3 *Are all abelian varieties with zero p-rank easy?*

Question 4 *Can one prove a theorem like theorem 1 with a sharper estimate for the running time namely* $q^{O(\gamma_i^a)}$ *with a smaller than* $1/2$*?*

References

[1] L.M. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over all prime fields. *Math. Comp.*, 61:1–155, 1993.

[2] L.M. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational sugroup of the jacobians of large genus hyperelliptic curves over finite fields. In *Proceedings of the first Algorithmic Number Theory Symposium*, volume 877 of *Lecture Notes in Computer Science*. Springer, 1994.

[3] Gilles Lachaud and Mireille Martin-Deschamps. Nombre de points des jacobiennes sur un corps fini. *Acta Arithmetica*, 56:329–340, 1990.

[4] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.

[5] Henri Lebesgue. *Leçons sur les constructions géométriques.* Gauthier-Villars, 1950.

[6] Jacques Martinet. *Les réseaux parfaits des espaces euclidiens.* Mathématiques. Masson, 1996.

[7] A. Menezes, T. Okamoto, and S.A Vanstone. Reducing elliptic curves logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[8] C. Pomerance. Fast, rigorous factorization and discrete logarithm algorithms. In *Discrete algorithms and complexity*, pages 119–143. Academic Press, 1987.

[9] Bjorn Poonen. Computational aspects of curves of genus at least 2. In *Proceedings of the second Algorithmic Number Theory Symposium*, volume 1122 of *Lecture Notes in Computer Science*. Springer, 1996.

[10] Maxwell Rosenlicht. Some basic theorems on algebraic groups. *Amer. J. of Math.*, 78:401–443, 1956.

[11] Jean-Pierre Serre. *Groupes algébriques et corps de classes*. Publications de l'institut de mathématiques de l'université de Nancago. Hermann, 1959.

[12] Henning Stichtenoth. *Algebraic function fields and codes*. Springer, 1993.