MATHEMATICS OF COMPUTATION
VOLUME 55, NUMBER 192
OCTOBER 1990, PAGES 745–763

FROBENIUS MAPS OF ABELIAN VARIETIES AND FINDING ROOTS OF UNITY IN FINITE FIELDS

J. PILA

"*If 'twere done when 'tis done, then 'twere well/ It were done quickly.*"–Macbeth.

ABSTRACT. We give a generalization to Abelian varieties over finite fields of the algorithm of Schoof for elliptic curves. Schoof showed that for an elliptic curve E over $\mathbf{F}_q$, given by a Weierstrass equation, one can compute the number of $\mathbf{F}_q$-rational points of E in time $O((\log q)^9)$. Our result is the following. Let A be an Abelian variety over $\mathbf{F}_q$. Then one can compute the characteristic polynomial of the Frobenius endomorphism of A in time $O((\log q)^{\Delta})$, where Δ and the implied constant depend only on the dimension of the embedding space of A, the number of equations defining A and the addition law, and their degrees. The method, generalizing that of Schoof, is to use the machinery developed by Weil to prove the Riemann hypothesis for Abelian varieties. By means of this theory, the calculation is reduced to ideal-theoretic computations in a ring of polynomials in several variables over $\mathbf{F}_q$. As applications we show how to count the rational points on the reductions modulo primes p of a fixed curve over $\mathbf{Q}$ in time polynomial in $\log p$; we show also that, for a fixed prime l, we can compute the lth roots of unity $\bmod p$, when they exist, in polynomial time in $\log p$. This generalizes Schoof's application of his algorithm to find square roots of a fixed integer $x \bmod p$.

1. INTRODUCTION

In this paper we generalize to Abelian varieties over finite fields the algorithm of Schoof [19] for elliptic curves over finite fields, and the application given by Schoof for his algorithm. Schoof showed that for an elliptic curve E over a finite field $\mathbf{F}_q$, given by a Weierstrass equation, one can compute the number of $\mathbf{F}_q$-rational points of E in time polynomial in $\log q$. The algorithm computes the characteristic polynomial $P(t) \in \mathbf{Z}[t]$ of the Frobenius endomorphism of E. For an elliptic curve, $P(t)$ is a monic, quadratic polynomial with constant term q, and the number of $\mathbf{F}_q$-rational points of E is $P(1)$. Our result is the following.

Theorem A. *Let A be an Abelian variety over a finite field $\mathbf{F}_q$, given explicitly as a projective variety with an explicit addition law. Then one can compute*

Received November 22, 1988; revised November 22, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11Y16, 11Y05, 14G15, 11G15.

the characteristic polynomial $P(t) \in \mathbf{Z}[t]$ *of the Frobenius endomorphism of* A *in time* $O((\log q)^{\Delta})$, *where* Δ *and the implied constant depend only on the dimension of the embedding space of* A, *the number of equations defining* A *and the addition law, and their degrees.*

The dependence on the form of the equations defining A corresponds to the Weierstrass equation in the elliptic curve case. The algorithm is described in §3, and its correctness is proved, while the running time is analyzed in §4. Adleman and Huang [1] have announced a nondeterministic generalization of Schoof's algorithm to curves of genus 2 as part of a random polynomial-time primality test. This primality test generalizes that of Goldwasser and Kilian [4], which employed Schoof's algorithm.

Applications. In the case that the Abelian variety A is the Jacobian variety of a curve C defined over $\mathbf{F}_q$, the zeta function of C is immediately recovered from $P(t)$, and in particular the number of $\mathbf{F}_q$-rational points of C. If C_0 is a smooth projective curve defined over $\mathbf{Q}$, we can construct, following Chow [3], the Jacobian variety J_0 of C_0 as a projective Abelian variety defined over $\mathbf{Q}$. Then, for all but finitely many primes p, the reduction J of J_0 modulo p is the Jacobian variety of the reduction C of C_0 modulo p. These Jacobians all have the same form of defining equations, so we have:

Theorem B. *Let* C_0 *be a smooth projective curve over* $\mathbf{Q}$. *There is a deterministic polynomial-time algorithm which on input* p *computes the zeta function of the reduction* C *of* C_0 *modulo* p, *hence, in particular, the number of* $\mathbf{F}_p$*-rational points of* C.

Here, polynomial-time means time polynomial in $\log p$. It should be possible to make Theorem B uniform for curves of a given genus. This entails showing that all curves of a given genus, over all fields (perhaps excluding a finite number of characteristics) can be presented by equations of the same form, and that their Jacobians can be uniformly constructed (with addition laws), again in the same form. We would thus do a precomputation for a given genus, rather than for a given curve over $\mathbf{Q}$. (For curves of genus 2, there is some recent work toward doing this explicitly, by D. Grant (*Formal groups in genus two*, preprint) and by Cassels and Flynn.)

Given a curve X_0 defined over $\mathbf{Q}$, but perhaps not smooth or projective, we can construct a smooth projective curve C_0 over $\mathbf{Q}$ birationally isomorphic to X_0 over $\mathbf{Q}$. The birational isomorphism persists between the reductions X and C of X_0 and C_0 modulo p for all but finitely many primes p. The $\mathbf{F}_p$-rational points of X and C are in bijective correspondence except at points corresponding to singular points or points at infinity. The adjustment for these points is easily made in polynomial time, and we obtain:

Theorem C. *Let* $f(x, y) \in \mathbf{Q}[x, y]$ *be absolutely irreducible. Then there is a deterministic polynomial-time algorithm which on input* p, *a prime number,*

computes the number of solutions to the congruence $f(x, y) \equiv 0 \bmod p$ *in* $\mathbf{F}_p \times \mathbf{F}_p$.

Schoof applied his algorithm to compute square roots of a fixed integer x modulo primes p, where they exist, in deterministic polynomial time. Given x, an elliptic curve defined over a number field is constructed. For those p with $(\frac{x}{p}) = 1$, $\sqrt{x} \bmod p$ is recovered from the characteristic polynomial of Frobenius of the reduction of this curve modulo p. Applying our algorithm to the Fermat curve

$$X^l + Y^l + Z^l = 0$$

over $\mathbf{Q}$, where l is a prime number, we obtain:

Theorem D. *Let* l *be an odd prime. There is a deterministic polynomial-time algorithm which on input* p *with* $p \equiv 1 \bmod l$ *(the condition that* l*th roots of unity exist modulo* p*) computes the* l*th roots of unity modulo* p*, and the prime ideals in* $\mathbf{Z}[\zeta_l]$ *lying over* (p).

Theorem D is proved in §5. Huang [9, 10] has shown that, assuming the Extended Riemann Hypothesis, the roots of $f(x) \equiv 0 \bmod p$, where p is a prime and $f(x)$ is an integral Abelian polynomial, can be found in deterministic polynomial time.

Method of proof of Theorem A. Our method generalizes the method of Schoof by appealing to the machinery developed by Weil [24, 25] to prove the Riemann hypothesis for curves and Abelian varieties. Our strategy is to compute the characteristic polynomial $P(t) \in \mathbf{Z}[t]$ of the Frobenius endomorphism ϕ of an Abelian variety A over $\mathbf{F}_q$ by computing $P(t) \bmod l$ for primes $l \leq H \log q$, where H is a constant such that, for all q,

$$\prod_{\substack{\text{primes } l \leq H \log q \\ (l, q)=1}} l > 2 \binom{2g}{g} q^g,$$

and g is the dimension of A. The desired H depends only on g and, from the prime number theorem, or indeed from the results of Chebyshev (see [5, p. 341]), it is easy to see that H is linear in g. Using explicit results of Rosser and Schoenfeld [18], we see that we can take $H = 9g + 3$. Since the coefficients of $P(t)$ are bounded in absolute value by $\binom{2g}{g} q^g$, the $P(t) \bmod l$ for $l \leq H \log q$ are sufficient to recover $P(t)$ using the Chinese remainder theorem.

For $(l, q) = 1$, $P(t) \bmod l$ is the characteristic polynomial of ϕ acting as an $\mathbf{F}_l$-linear transformation of the l-torsion points $A[l]$ of A. We know that $A[l]$ is a $2g$-dimensional vector space over $\mathbf{F}_l$. We check the action of polynomials in ϕ on $A[l]$ by explicit ideal-theoretic computations with their defining ideals. Schoof's algorithm reduces to ideal-theoretic computations in the ring of polynomials in one variable over $\mathbf{F}_q$; we must operate in the ring of polynomials in several variables. For each l, we obtain explicit expressions for the multiplication by n maps on A for $n = 2, \ldots, l$, and a definition of $A[l]$ as a

zero-dimensional algebraic set. In order that ideal membership be equivalent to vanishing on the algebraic set, we must ensure that our ideals are radical. The action of Frobenius is given by polynomials of degree q. We cannot operate with these, but must find low-degree equivalents to these polynomials on $A[l]$ by repeated squaring and reduction modulo the ideal defining $A[l]$.

Unlike the elliptic curve case, the characteristic polynomial may not be immediately recoverable from the minimal polynomial. To determine the powers of irreducible polynomials $r(t)$ occurring in $P(t) \bmod l$, we count the number of points in the kernels of powers of $r(\phi)$ as transformations on $A[l]$. To count the points, we test linear independence of monomials with respect to an ideal. Not having a division algorithm as in the one-variable case, we must appeal to explicit bounds for ideal membership to reduce to systems of linear equations over $\mathbf{F}_q$.

Beyond establishing a running time bound polynomial in $\log q$, we have not attempted to make the algorithm as efficient as possible, and it seems that considerably more work would be needed to make it amenable to implementation. A further difficulty is the lack of examples of explicitly defined Abelian varieties to serve as input. (For dimension 2, there is the aforementioned work of D. Grant, and Cassels and Flynn.) In the applications we give, Abelian varieties over finite fields are obtained by reduction of Abelian varieties defined over $\mathbf{Q}$. The latter can then be obtained by constructions taking a bounded amount of time, independent of p, such as the construction of the Jacobian variety of a curve over $\mathbf{Q}$. Here we have appealed to the construction of Chow [3] which, while possible in principle, is extremely impractical, even for curves of small genus. As a result, the algorithms in Theorems B, C, and D are extremely impractical in their present form. A possible alternative to projective Abelian varieties would be *abstract* Abelian varieties (see Weil [27] for the definition of abstract variety). Apart from being easier to construct, the constituent affine varieties would be embedded in spaces of much smaller dimension.

2. Preliminaries

Algebraic geometry. Our notation and terminology is mostly standard, and can be found in Hartshorne [6], Shafarevich [21], or Silverman [22]. We also introduce some notation for moving between affine and projective varieties, and for explicit presentation of rational maps.

Let K be a field with algebraic closure $\overline{K}$. *Affine n-space over* K is denoted $\mathbf{A}^n$ or $\mathbf{A}^n(\overline{K})$. If I is an ideal in $\overline{K}[X]$, where $X = (X_1, \ldots, X_n)$, then $V(I)$ denotes the associated *affine algebraic set* in $\mathbf{A}^n$. An affine algebraic set V is *defined over* K if the associated ideal $I(V)$ in $\overline{K}[X]$ can be generated by elements of $K[X]$. If V is defined over K, the set of *K-rational points* of V is denoted $V(K)$. If V is an affine algebraic set, the *coordinate ring* of V over K is

$$K[V] = K[X]/I(V) \cap K[X].$$

An affine algebraic set V is an *affine variety* if $I(V)$ is a prime ideal in $\overline{K}[X]$.

Projective n-space over K is denoted $\mathbf{P}^n$ or $\mathbf{P}^n(\overline{K})$. Let $X = (X_0, \ldots, X_n)$. If I is a homogeneous ideal in $\overline{K}[X]$, then $V(I)$ denotes the associated *projective algebraic set* in $\mathbf{P}^n(\overline{K})$. A projective algebraic set V is *defined over* K if the associated homogeneous ideal $I(V)$ can be generated by forms in $K[X]$. If V is defined over K, the set of *K-rational points* of V is denoted $V(K)$. A projective algebraic set V is called a *projective variety* if $I(V)$ is a prime ideal in $\overline{K}[X]$.

If $X = (X_0, \ldots, X_n)$ and i is in the range $0, \ldots, n$, we let $(X)_i$ denote the n-tuple $(X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$. We view $(X)_i$ as coordinates of $\mathbf{A}^n$. If $F(X) \in K[X]$, we set

$$F(X)_i = F(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n) \in K[(X)_i].$$

We denote $K[(X)_i]$ by $K[X]_i$. If $I \subset K[X]$ is an ideal generated by $F_1(X), \ldots, F_m(X)$, we let I_i be the ideal in $K[X]_i$ generated by $F_1(X)_i, \ldots, F_m(X)_i$. If $V = V(I)$ is a projective algebraic set, we let V_i denote the affine algebraic set $V(I_i)$ in $\mathbf{A}^n$.

Let V, W be projective varieties in $\mathbf{P}^n$, $\mathbf{P}^m$ respectively. A *rational map* $\psi : V \to W$ is a map of the form

$$\psi = (\psi_0, \ldots, \psi_m),$$

where $\psi_i \in \overline{K}[X]$ are forms of the same degree, not all in $I(V)$, with the property that for each $F \in I(W)$, $F(\psi_0(X), \ldots, \psi_m(X)) \in I(V)$. We say that ψ is *defined* at a point $P \in V$ if there exist forms $\theta_0, \ldots, \theta_m \in \overline{K}[X]$ of the same degree such that

(i) $\psi_i\theta_j \equiv \psi_j\theta_i \bmod I(V)$ for all i and j, and
(ii) $\theta_j(P) \neq 0$ for some j.

If ψ is defined at $P \in V$ and the forms θ_i have the above properties, we set

$$\psi(P) = (\theta_0(P), \ldots, \theta_m(P)).$$

A rational map $\psi: V \to W$ that is defined at all points of V is called a *morphism.*

Suppose $\psi: V \to W$ is a rational map of projective varieties. An m-tuple of forms $(\theta_0, \ldots, \theta_m)$, $\theta_i \in \overline{K}[X]$ of the same degree, is called a *chart* for ψ if

(i) $\psi_i\theta_j = \psi_j\theta_i \bmod I(V)$ for all i and j, and
(ii) $\theta_i \notin I(V)$ for some i.

There is a finite set of charts $L_1, \ldots, L_r$, $L_i = (\theta_0^i, \ldots, \theta_m^i)$, with the property that if $P \in V$ and ψ is defined at P, there is an L_i such that $\theta_j^i(P) \neq 0$ for some j. Such a set of charts is called an *atlas* for ψ. We say that ψ is defined over K if V and W are defined over K and ψ has an atlas consisting of forms in $K[X]$. This happens if and only if ψ has a chart

consisting of forms in $K[X]$. For varieties in $\mathbf{P}^n \times \mathbf{P}^m$, rational maps and charts are given by systems of bihomogeneous polynomials.

Suppose that $V \subset \mathbf{P}^n$ and $W \subset \mathbf{P}^m$ are projective varieties, and ψ and ψ' are morphisms from V to W with atlases M and M'. Then the symbol $[M, M']$ will denote the set of all expressions

$$L_i(X)L'_j(X) - L_j(X)L'_i(X),$$

where i, j range over $0, \ldots, m$, $(L_0, \ldots, L_m)$ is a chart of ψ belonging to M and $(L'_0, \ldots, L'_m)$ is a chart of ψ' belonging to M'. Thus, if $V = V(I)$, the ideal $(I, [M, M'])$ determines the subset of V of points P with $\psi(P) = \psi'(P)$. If Q is a point of W, then we also denote by Q the atlas for the constant map $V \to W$ consisting of the single chart $(Q_0, \ldots, Q_m)$.

Abelian varieties. Here we refer to any of the following: Weil [25], Lang [12], Milne [16], Mumford [17]. A *(projective) Abelian variety* A is a projective variety A together with a distinguished point $E \in A$, and morphisms

$$\psi : A \times A \to A, \qquad \theta : A \to A$$

such that A is a group with identity element E, composition law $x \cdot y = \psi(x, y)$, and such that $\theta(x) = x^{-1}$. We say that A is defined over K if A is defined over K as a projective variety, E is a K-rational point of A, and the morphisms ψ and θ are defined over K. An Abelian variety of dimension 1 is an elliptic curve. If A is an Abelian variety, then the projective variety A is *smooth*, and the group A is commutative.

Let A, B be Abelian varieties. By a *homomorphism* of A into B we will mean a morphism that is a group homomorphism. An *isogeny* is a homomorphism whose kernel is finite. An *endomorphism* of A is a homomorphism of A into itself.

Let A be an Abelian variety of dimension g defined over a field K. Since A is an Abelian group, we let $+$ denote the group law on A. Let l be a prime distinct from $\operatorname{char} K$. Then the map $l: A \to A$, $P \to lP = P + \cdots + P$ for $P \in A$ is clearly an endomorphism. It is also an isogeny. It is also separable, unramified, and of degree l^{2g}, so that for any m, the kernel $A[l^m]$ of the map l^m consists of l^{2gm} points. The inverse limit of the $A[l^m]$ under the l map is called the Tate module and is denoted by $T_l A$. It is a free module over the l-adic integers $\mathbf{Z}_l$ of rank $2g$. The tensor product $T_l A \otimes \mathbf{Q}_l$ is a vector space over $\mathbf{Q}_l$ of dimension $2g$.

Let A be an Abelian variety defined over a finite field $\mathbf{F}_q$ of characteristic p. Let ϕ be the Frobenius map of $\overline{\mathbf{F}}_q$, that is, the map $x \to x^q$. Then ϕ extends to a map $\phi: \mathbf{P}^N \to \mathbf{P}^N$, where $\phi(x_0, \ldots, x_N) = (x_0^q, \ldots, x_N^q)$. Since A is defined over $\mathbf{F}_q$, ϕ restricts to a map $\phi: A \to A$. This map is a morphism, and also a group homomorphism since the addition law on A is defined over $\mathbf{F}_q$ and $E \in A(\mathbf{F}_q)$; it is called the *Frobenius endomorphism* of A and denoted ϕ. Clearly, ϕ restricts to an automorphism of each $A[l^m]$, commuting with

the maps $n: A \to A$ for any integer n, and hence induces a vector space transformation of $T_l A \otimes \mathbf{Q}_l$ over $\mathbf{Q}_l$, which we also denote ϕ.

Let $P(t)$ be the characteristic polynomial of ϕ as an endomorphism of $T_l A \otimes \mathbf{Q}_l$. Then $P(t)$ is monic of degree $2g$, has rational integral coefficients, and is independent of l for $l \neq p$; indeed, $P(t)$ can be characterized independently of l by the property that $P(n) = \deg(\phi - n)$ for all $n \in \mathbf{Z}$. By the Riemann hypothesis for Abelian varieties (Weil [25]) the roots of $P(t)$ in $\mathbf{C}$ have modulus $\sqrt{q}$.

We will compute $P(t)$ by computing $P(t) \bmod l$ for small $l \neq p$. For such l, ϕ acts as a vector space transformation of $A[l]$ over $\mathbf{F}_l$. Let $P_l(t)$ be the characteristic polynomial of this transformation.

Proposition 2.1. *Suppose $l \neq p$. Then $P_l(t) \equiv P(t) \bmod l$.*

Proof. Let $\{x_1, \ldots, x_{2g}\}$ be a basis for $T_l A$ over $\mathbf{Z}_l$. Then $\{x_1, \ldots, x_{2g}\}$ is a basis of $T_l A \otimes \mathbf{Q}_l$ over $\mathbf{Q}_l$. Since $\phi(A[l^m]) \subset A[l^m]$ for each m, the matrix M_ϕ of ϕ with respect to this basis has entries belonging to $\mathbf{Z}_l$. The action of ϕ on $A[l]$ is represented by the matrix $M_\phi \bmod l$. □

Ideal theory. Let K be a field, $\overline{K}$ an algebraic closure of K, and $X = (X_1, \ldots, X_n)$ a system of indeterminates. Let I be an ideal of $K[X]$. From the decomposition theory of ideals in Noetherian rings [23], there is a least positive integer e with the property that, for all $f \in K[X]$, if some power f^n lies in I, then $f^e \in I$. This e is called the *exponent* of I, and denoted $e_K(I)$. An ideal of exponent one is called *radical*. An ideal I is called *zero-dimensional* if the affine algebraic subset $V(I)$ of $\mathbf{A}^n(\overline{K})$ determined by I consists of a finite set of points.

Proposition 2.2. *Suppose that L is an extension field of K, $f, f_1, \ldots, f_r \in K[X]$. If $f = \sum \alpha_i f_i$ for some $\alpha_i \in L[X]$, then $f = \sum \beta_i f_i$ for some $\beta_i \in K[X]$. Moreover, the monomials occurring in the β_i all appear in the α_i.*

Proof. This is elementary linear algebra and can be found in [23, 16.7]. □

For an ideal I in $K[X]$, we denote by $\overline{I}$ the ideal generated by I in $\overline{K}[X]$. From the above proposition it follows that if I and J are ideals in $K[X]$, then $I \subset J$ if and only if $\overline{I} \subset \overline{J}$. In writing relations of containment between ideals we can therefore suppress mention of the field.

Proposition 2.3. *Let I be an ideal in $K[X]$. Then $e_K(I) \leq e_{\overline{K}}(\overline{I})$.*

Proof. This is immediate from Proposition 2.2 and the least integer characterization of the exponent. □

If $a = (a_1, \ldots, a_n)$ is a point in $\mathbf{A}^n(\overline{K})$, let P_a denote the ideal generated by $X_i - a_i$, $i = 1, \ldots, n$, in $\overline{K}[X]$.

Proposition 2.4. *Suppose that I is zero-dimensional and that $P_a^\sigma \subseteq (I, P_a^{\sigma+1})$ for each $a \in V(I)$. Then $e_{\overline{K}}(\overline{I}) \leq \sigma$.*

Proof. This is a corollary of Noether's theorem in [23, 16.7]. □

Theorem 2.5. *Let V, W be smooth projective varieties defined over K and of the same dimension, and let $\theta: V \to W$ be a finite morphism defined over K, given by an atlas M, and unramified at a point $R \in W$ (meaning that R has precisely $\deg\theta$ inverse images in V). Suppose that $i \in \{0, \dots, n\}$, and that I is an ideal in $K[X]_i$ with $\overline{I} = I(V_i)$. Then the ideal $(I, [M, R]_i)$ is radical.*

Proof. In view of Propositions 2.4 and 2.3, it suffices to show that for each point $Q \in V_i$ with $\theta(Q) = R$ we have

$$P_Q \subseteq (I, [M, R]_i, P_Q^2).$$

Note that if there are no such points Q, then $(I, [M, R]_i) = K[X]_i$ by the Nullstellensatz, and is certainly radical. Choose j such that $R_j \neq 0$, and so $R \in W_j$. Let $M_Q = \{F \in K[V_i] : F(Q) = 0\}$, and let M_R be the corresponding ideal in $K[W_j]$. Then the above is equivalent to the surjectivity of the induced map $\theta^*: M_R/M_R^2 \to M_Q/M_Q^2$. That this map is an isomorphism of vector spaces follows from the hypothesis that θ is unramified at Q (see [21, Theorem II.5.8]). □

Theorem 2.6. *Suppose I is a zero-dimensional radical ideal in $K[X]$ with zero set V in $\mathbf{A}^n(\overline{K})$. Clearly, $K[X]/I$ is a vector space over K. The dimension of $K[X]/I$ over K is $|V|$, and there is a basis of monomials of degree at most $|V|$.*

Proof. If x, y are distinct points of V, there is a linear $f \in \overline{K}[X]$ with $f(x) = 1$, $f(y) = 0$. Hence, for $x \in V$ there is an $f \in \overline{K}[X]$ of total degree at most $|V| - 1$ such that $f(x) = 1$, $f(y) = 0$ for $y \in V - \{x\}$. The $|V|$ such functions are clearly a basis for $\overline{K}[X]/\overline{I}$ over $\overline{K}$, so the monomials occurring in them, which are of degree at most $|V|$, span $\overline{K}[X]/\overline{I}$ over $\overline{K}$. The monomials forming the basis of $\overline{K}[X]/\overline{I}$ over $\overline{K}$ are linearly independent in $K[X]/I$ over K. By Proposition 2.2 they also span. □

The following theorem has a long history, of which we mention the papers by Hilbert [8], Hermann [7], Seidenberg [20], and Mayr and Meyer [15].

Theorem 2.7. *Let K be a field, and F_{ij}, $B_i \in K[X]$ for $i = 1, \dots, t$, $j = 1, \dots, s$, where $X = (X_1, \dots, X_n)$. Suppose d bounds the degrees of the F_{ij}, and b bounds the degrees of the B_i. Then the system of linear equations*

$$\sum_{j=1}^{s} F_{ij} G_j = B_i, \qquad i = 1, \dots, t,$$

has a solution $(G_1, \dots, G_s)$, $G_i \in K[X]$, if and only if it has a solution comprising polynomials $G_j \in K[X]$ with $\deg G_j \leq b + (sd)^{2^n}$.

Proof. We first observe, following [20], that we can assume that K is infinite. We now follow the exposition in [15]. Although the result there is stated only over $\mathbf{Q}$, the only use made of this is to enable regularization of polynomials. This can be done whenever K is infinite. □

We appeal to this theorem in the special case of membership in a zero-dimensional radical ideal, in which situation better bounds than these may be available.

3. The algorithm

In this section we describe the algorithm of Theorem A and prove its correctness. The next section establishes the asserted running time. Let A be an Abelian variety over a finite field $\mathbf{F}_q$. We suppose A to be given in the following explicit form:

1. Forms $F_1(X), \dots, F_S(X) \in \mathbf{F}_q[X]$, $X = (X_0, \dots, X_N)$, defining A as a projective variety in $\mathbf{P}^N$ over $\mathbf{F}_q$. We assume that, for each i, the ideal $(F_1, \dots, F_S)_i$ is radical. Let
$$T = \max\{\deg F_j(X) : j = 1, \dots, S\}.$$
2. An atlas for the addition law on A, consisting of R charts
$$G^{(i)}(X, Y), \qquad i = 1, \dots, R,$$
$$G^{(i)}(X, Y) = (G_0^{(i)}(X, Y), \dots, G_N^{(i)}(X, Y)),$$
where $Y = (Y_0, \dots, Y_N)$, and $G_j^{(i)}(X, Y) \in \mathbf{F}_q[X, Y]$ are homogeneous of the same degree D in each system of variables.
3. The identity element E of A as a point in $A(\mathbf{F}_q)$.
4. The dimension g of A. A bound on the dimension is enough, and the dimension N of the embedding space is clearly such a bound.

Our strategy is to compute the characteristic polynomial $P(t) \in \mathbf{Z}[t]$ of the Frobenius endomorphism of A by computing $P(t) \bmod l$ for many small l. As remarked in §1, the $l \le H \log q$, where $H = 9g + 3$, suffice for this purpose. Note that, as remarked by Schoof [19], while we have appealed to the Riemann hypothesis for Abelian varieties to bound the coefficients of $P(t)$, trivial bounds would suffice.

We proceed to describe the subalgorithm to be followed for each $l \le H \log q$, $(l, q) = 1$. In order that the entire algorithm run in time polynomial in $\log q$, it suffices that the subalgorithm run in time polynomial in l.

According to Proposition 2.1, $P(t) \bmod l$ coincides with $P_l(t)$, the characteristic polynomial of ϕ as a vector space transformation of $A[l]$. The polynomial $P_l(t)$ has a factorization
$$P_l(t) = \prod r_i(t)^{m_i}$$
with $r_i(t) \in \mathbf{F}_l[t]$ distinct, monic, and irreducible, and with
$$\sum m_i \deg r_i = \deg P_l = 2g.$$
For each i, $m_i \deg r_i$ is the $\mathbf{F}_l$-dimension of the largest kernel of the maps $r_i(\phi)^j$, $j = 1, 2, \dots$, with $j \cdot \deg r_i \le 2g$ as a subspace of $A[l]$. To compute the dimension of the kernel of a map $r(\phi)$ on $A[l]$, we compute the number of

points in the kernel. For this we will use Theorem 2.6. Note that these kernels contain at most l^{2g} points, and $l \ll \log q$.

We begin by obtaining a list of the monic irreducible polynomials $s(t) \in \mathbf{F}_l[t]$ of degree $\leq 2g$, and the largest powers $r(t)$ of these of degree $\leq 2g$. To obtain this, we can simply list the l^{2g} possible polynomials and test them for irreducibility. We will describe a further subalgorithm to be carried out for each $r(t)$, but must first make some more preparations.

We must generate atlases $M_1, \ldots, M_l$ for the maps $1, \ldots, l: A \to A$ in such a way that the number of charts comprising M_n, and the degrees of the forms comprising the charts, are polynomial in n. Let M_1 consist of the single $(N+1)$-tuple $X = (X_0, \ldots, X_N)$; M_1 is then an atlas for the identity map $1: A \to A$. We now set recursively

$$M_{2n} = \{G^{(i)}(L(X), L(X)) : i = 1, \ldots, R, \ L \in M_n\},$$
$$M_{2n+1} = \{G^{(i)}(L(X), G^{(j)}(L(X), X)) : i, j = 1, \ldots, R, \ L \in M_n\},$$

and establish the properties required.

Proposition 3.1. *The number of charts $|M_n|$ in M_n is less than or equal to $R^{2\log_2 n} = n^{2\log_2 R}$.*

Proof. We use induction on n, where the case $n = 1$ is trivial. Suppose $|M_n| \leq R^{2\log_2 n}$. Then

$$|M_{2n}| \leq RR^{2\log_2 n} \leq R^{2\log_2 2n},$$
$$|M_{2n+1}| \leq R^2 R^{2\log_2 n} \leq R^{2\log_2(2n+1)},$$

completing the induction and the proof. □

Let D_n be the maximum degree of a form in M_n. Then we see immediately that

$$D_{2n} \leq 2DD_n, \qquad D_{2n+1} \leq DD_n + D^2 D_n + D^2,$$

so that $D_n \leq p_n(D)$, where the $p_n(x)$ are polynomials defined recursively by

$$p_1(x) = 1,$$
$$p_{2n}(x) = 2xp_n(x),$$
$$p_{2n+1}(x) = xp_n(x) + x^2 p_n(x) + x^2.$$

Proposition 3.2. *We have $D_n \leq n^{1+2\log_2 D}$.*

Proof. The polynomials $p_n(x)$ have positive coefficients, and D is positive, so that, if d_n is the degree of $p_n(x)$, we have

$$D_n \leq p_n(D) \leq D^{d_n} p_n(1).$$

Now $p_n(1) = n$ trivially by induction, while the d_n satisfy $d_1 = 0$, $d_{2n} = d_n + 1$, $d_{2n+1} = d_n + 2$, so that, by induction, $d_n \leq 2\log_2 n$. □

Using M_l, we have an ideal in $\mathbf{F}_q[X]$ determining the l-torsion points of A:

$$A[l] = V(F_1, \ldots, F_S, [M_l, E]).$$

The notation [,] is defined in §2. Since the affine ideals $(F_1, \ldots, F_S)_i$, $i = 0, \ldots, N$, are radical by hypothesis, and the map $l: A \to A$ is finite and unramified (since $(l, q) = 1$), we conclude by Theorem 2.5 that the ideals

$$(F_1, \ldots, F_S, [M_l, E])_i, \qquad i = 0, \ldots, N,$$

are zero-dimensional and radical.

For each $i = 0, \ldots, N$ we desire a monomial basis for the $\mathbf{F}_q$ vector space,

$$\mathbf{F}_q[A[l]_i] = \mathbf{F}_q[X]_i/(F_1, \ldots, F_S, [M_l, E])_i.$$

Since

$$|A[l]_i| \leq |A[l]| = l^{2g},$$

we know by Theorem 2.6 that the monomials in $(X)_i$ of degree $\leq l^{2g}$ span $\mathbf{F}_q[A[l]_i]$ over $\mathbf{F}_q$. We reduce this spanning set to a basis by testing linear dependence with respect to the ideal $(F_1, \ldots, F_S, [M_l, E])_i$. To test the dependence of a monomial m on monomials $m_1, \ldots, m_r$ we appeal to the explicit bounds for ideal membership of Theorem 2.7 and try to solve the linear inhomogeneous system

$$m - \sum \alpha_k m_k = \sum b_j f_j,$$

where the f_j generate $(F_1, \ldots, F_S, [M_l, E])_i$, $\alpha_k \in \mathbf{F}_q$, and $b_j \in \mathbf{F}_q[X]_i$ with

$$\deg b_j \leq l^{2g} + ((S + N|M_l|) \max(T, D_l))^{2^N}.$$

This system has at most

$$(1 + l^{2g} + ((S + N|M_l|) \max(T, D_l))^{2^N} + \max(T, D_l))^N$$

equations (one for each monomial up to the total degree of the equation) in at most

$$(1 + l^{2g} + ((S + N|M_l|) \max(T, D_l))^{2^N})^N (S + N|M_l|) + l^{2g}$$

unknowns (one for each coefficient of each b_j, and up to l^{2g} for the α_k), and hence is a system of size polynomial in l.

By repeated squaring and reduction with respect to the basis of $\mathbf{F}_q[A[l]_i]$ we obtain the low-degree polynomials equivalent on $A[l]_i$ to the powers of Frobenius: $\phi, \ldots, \phi^{2g}$, that is, to the polynomials $X_j^{q^k}$ for $k = 1, \ldots, 2g$, $j \neq i$, $i = 0, \ldots, N$.

Now suppose that $r(t) \in \mathbf{F}_l[t]$ is monic of degree $\leq 2g$. For each $i = 0, \ldots, N$, we write down an atlas $M(r, i)$ for $r(\phi)$ on $A[l]_i$, using the low-degree equivalents of ϕ^j. By Theorem 2.5, for each i, the ideal

$$(F_1, \ldots, F_S, [M_l, E], [M(r, i), E], X_j : j < i)_i$$

is zero-dimensional and radical. The number of points in its zero set can be computed by further reducing the basis of $\mathbf{F}_q[A[l]_i]$. For different i, the zero sets are disjoint, and the union over i gives the set of points $P \in A[l]$ with $r(\phi)P = E$. This completes the description of the algorithm.

4. Running time

To operate in $\mathbf{F}_q$, we assume given an irreducible polynomial $f(x) \in \mathbf{F}_p[x]$ of degree $[\mathbf{F}_q : \mathbf{F}_p]$. The operation of the algorithm involves basically four kinds of activities:

1. Polynomial arithmetic, including substitution of polynomials into other polynomials. This occurs in the formation of atlases for rational maps, in conjunction with reduction modulo ideals.
2. Testing ideal membership. This entails solving linear inhomogeneous systems over $\mathbf{F}_q$. These tests occur at several points in the algorithm.
3. Finding all irreducible polynomials of degree $\leq 2g$ in $\mathbf{F}_l[t]$ for $l \leq H \log q$, and the highest powers of these of degree $\leq 2g$.
4. Recovery of $P(t)$ from $P_l(t)$ by means of the Chinese remainder theorem.

Among these operations, the solution of the linear inhomogeneous systems associated with the ideal membership determinations dominate in number of required field operations in $\mathbf{F}_q$, and we restrict our attention to them. Ideal membership tests arise at five points in the algorithm:

1. Computing monomial bases of $\mathbf{F}_q[A[l]]_i$.
2. Obtaining low-degree equivalents to Frobenius.
3. Obtaining low-degree atlases for the maps $\alpha\phi^m$, $\alpha \in \mathbf{F}_l$.
4. Obtaining low-degree atlases for $r(\phi)$, $r(t) \in \mathbf{F}_l[t]$.
5. Counting the points in the kernel of $r(\phi)$ on $A[l]_i$.

We will examine each of these to determine the parameters of the linear systems involved in each, and how many times we must solve such a system. All the ideal membership determinations are in the ring of polynomials in N variables over $\mathbf{F}_q$, where N is the embedding space dimension of A. According to Theorem 2.7, $B \in (F_1, \ldots, F_r)$, where $B, F_i \in \mathbf{F}_q[X]$, $X = (X_1, \ldots, X_N)$, if and only if $B = \sum F_i G_i$ with

$$\deg G_i \leq b + (rd)^{2^n},$$

where $\deg B \leq b$ and $\deg F_i \leq d$. We will bound the parameters b, d, r and the number of iterations m in each of the above situations. The linear inhomogeneous system arising from $B = \sum F_i G_i$ has at most

$$(1 + b + (rd)^{2^N} + d)^N$$

equations in at most $(1+b+(rd)^{2^N})^N \cdot r$ unknowns. In the tests of monomial dependence, the coefficients of B contribute additionally at most l^{2g} unknowns.

Thus the size of the linear system involved is at most

$$r \cdot (1 + b + (rd)^{2^N} + d)^N + l^{2g},$$

and the solubility or solutions can be obtained in $O((\text{size})^3)$ elementary operations.

1. *Computation of monomial bases.* We must compute a monomial basis of $\mathbf{F}_q[A[l]]_i$ for each $l \leq H \log q$, and each $i = 0, \ldots, N$. We begin with a spanning set of l^{2gN} monomials, each of degree $\leq l^{2g}$. The ideal defining $A[l]_i$ is generated by at most $r = S + N|M_l|$ polynomials. For the other parameters, we have $b = l^{2g}$, $d = \max\{T, D_l\}$, and $m = H(\log q)(N+1)l^{2gN}$.

2. *Low-degree equivalents to Frobenius.* We must find low-degree ($\leq l^{2g}$) equivalents of the polynomials $X_j^{q^k}$ on $A[l]_i$ for $l \leq H \log q$, $i = 0, \ldots, N$, $k = 1, \ldots, 2g$, $j \neq i$. It is trivial by induction that we can compute x^n from x in at most $2 \log_2 n$ multiplications. Performing a reduction to a polynomial of degree $\leq l^{2g}$ with respect to the ideal of $A[l]_i$ between each of these gives us

$$m = H(\log q)(N+1)2g \cdot N \cdot 2 \log_2(q^{2g}),$$
$$b = l^{4g}, \qquad d = \max\{T, D_l\}, \qquad r = S + N|M_l|.$$

3. *Low-degree atlas of $\alpha\phi^n$.* Compute, for each l, a low-degree atlas of $\alpha\phi^m$ on $A[l]_i$ for each i, $m = 1, \ldots, 2g$, for each $\alpha \in \mathbf{F}_l$. We must substitute the low-degree equivalents to ϕ^m into M_α, the atlas for α. Since M_α has $|M_\alpha|$ charts, each with $N+1$ coordinate functions, we have

$$m = H(\log q)(N+1)2g \cdot l \cdot |M_*| \cdot (N+1),$$
$$b = l^{2g} D_l, \qquad d = \max\{T, D_*\}, \qquad r = S + N|M_*|,$$

where $|M_*|$ bounds the $|M_\alpha|$ for $\alpha \in \mathbf{F}_l$, and D_* bounds the D_α for $\alpha \in \mathbf{F}_l$.

4. *Low-degree atlas of $r(\phi)$.* We add the terms of the form $\alpha\phi^m$, reducing as we go. The number of charts increases with each of the $2g$ additions. Thus we have

$$m = H(\log q)l^{2g}(N+1)(N+1) \cdot \sum (R|M_*|^2 + R^2|M_*|^3 + \cdots + R^{2g+1}|M_*|^{2g+2}),$$
$$b = l^{2g}, \qquad d = \max\{T, D_*\}, \qquad r = S + N|M_*|.$$

5. *Counting kernel of $r(\phi)$ on $A[l]_i$.* We must add generators to the ideal of $A[l]_i$ to get the ideal of the kernel; thus,

$$r = S + N|M_l| + NR^{2g+1}|M_*|^{2g+2}.$$

For each l, $r(\phi)$, and i, we must reduce a spanning set of l^{2g} monomials to a basis. As there are up to l^{2g} polynomials $r(t)$, we have

$$m = H(\log q)(N+1)l^{4g}, \qquad d = \max\{T, D_l, l^{2g}\}, \qquad b = l^{2g}.$$

From Propositions 3.1 and 3.2 we can take

$$|M_l|, |M_*| \leq l^{2\log_2 R}, \qquad D_l, D_* \leq l^{1+2\log_2 D}.$$

This gives a running time bound of the desired form $O((\log q)^{\Delta})$, where Δ and the implied constant depend on the parameters N, S, T, R, D, g. We note that

$$\Delta \leq 6(2g+2)(2\log R)\cdot \max\{2g, 1+2\log D\}\cdot N2^N$$

is independent of S and T. This completes the proof of Theorem A, and hence also of Theorems B and C, as indicated in the introduction.

5. Finding roots of unity in finite fields

In this section we prove Theorem D. Let l be an odd prime. Write $l = 2m+1$. Let $\psi(x)$ be the lth cyclotomic polynomial, and ζ_l a root of $\psi(x)$ in $\mathbf{C}$. The following statements are equivalent:

1. The prime ideal (p) in $\mathbf{Z}$ splits completely in $\mathbf{Z}[\zeta_l]$.
2. $\psi(x)$ factors completely in $\mathbf{F}_p[x]$.
3. $p \equiv 1 \bmod l$.

We consider the following problems:

Problem A. Given l, p with $p \equiv 1 \bmod l$, find the $2m$ primes lying over (p) in $\mathbf{Z}[\zeta_l]$.

Problem B. Given l, p with $p \equiv 1 \bmod l$, factor $\psi(x)$ in $\mathbf{F}_p[x]$.

As is easily shown, these problems are polynomial time equivalent. More generally, Huang [9] shows that factoring polynomials of degree n in $\mathbf{F}_p[x]$ is polynomially equivalent to factoring (p) in algebraic number fields of degree n, where p is regular with respect to the generating polynomials.

Our method is based on Jacobi sums, which we can compute in time polynomial in $\log p$ via the characteristic polynomial of the Frobenius endomorphism of the Jacobian variety of the Fermat curve. We show that the prime ideals over (p) are generated by certain combinations of Jacobi sums, and the algorithm is simply an exhaustive search over the appropriate combinations. The verification of a correct choice is accomplished by checking that we have found the lth roots of unity $\bmod p$. In this way, we solve both Problems A and B simultaneously.

Equivalence of Problems A and B. Given the factorization $\prod(x-a_i)$ of $\psi(x)$ in $\mathbf{F}_p$, the primes above (p) are $(p, \zeta_l - a_i)$. Conversely, suppose we are given that $(u_1, \ldots, u_k)$ is a prime lying over (p), where $u_i \in \mathbf{Z}[\zeta_l]$. Write $u_i = h_i(\zeta_l)$, where $h_i(x) \in \mathbf{Z}[x]$, $\deg h_i(x) \leq l-2$. Since (p) splits completely, and $p \in (u_1, \ldots, u_k)$, we have

$$\mathbf{F}_p \cong \frac{\mathbf{Z}[\zeta_l]}{(p, u_1, \ldots, u_k)} \cong \frac{\mathbf{F}_p[x]}{(h_1(x), \ldots, h_k(x), \psi(x))}$$
$$\cong \frac{\mathbf{F}_p[x]}{\gcd(h_1(x), \ldots, h_k(x), \psi(x))}.$$

Hence, the gcd must be linear. That is,

$$\gcd(h_1(x), \ldots, h_k(x), \psi(x)) = x - a$$

for some $a \in \mathbf{F}_p$, which is then a primitive lth root of unity.

Jacobi sums. Here we follow [11, pp. 4–13]. Let G be the Galois group of $\mathbf{Q}(\zeta_l)$ over $\mathbf{Q}$. Then G is cyclic of order $l-1$. We identify G with the multiplicative group $\mathbf{F}_l^*$ by denoting the elements of G as σ_c, $c \in \mathbf{F}_l^*$, where $\sigma_c \zeta_l = \zeta_l^c$. Let e be a generator of $\mathbf{F}_l^*$, so that $G = \{\sigma_{e^i} : i = 0, \ldots, l-1\}$. As is well known, G acts transitively on the primes of $\mathbf{Z}[\zeta_l]$ above (p). Since (p) splits completely, the number of primes above (p) is $l-1$, the order of G. So if P_i, P_j are primes above (p), there is a unique $c \in \mathbf{F}_l^*$ such that $\sigma_c P_i = P_j$.

For N an integer, let μ_N denote the group of Nth roots of unity in $\mathbf{C}$. If $\chi_1, \chi_2 \colon \mathbf{F}_p^* \to \mu_{p-1}$ are characters, define $\chi_i(0) = 0$ and set

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbf{F}_p} \chi_1(x)\chi_2(1-x).$$

J is called a *Jacobi sum*. Let P be a prime in $\mathbf{Z}[\zeta_l]$ over (p), and let $\chi = \chi_P$ be a character of $\mathbf{F}_p^*$ determined by

$$\chi(a) \equiv a^{-(p-1)/l} \mod P.$$

Note that $a^{-(p-1)/l}$ is an lth root of unity in $\mathbf{F}_p$. Thus, χ generates the group of characters $\mathbf{F}_p^* \to \mu_l$.

Let $\langle t \rangle$ denote the fractional part of a real number t, with $0 \le \langle t \rangle < 1$. For an integer d, we let $[d]\langle t \rangle = \langle dt \rangle$. Also set $\Delta[a, b] = [a] + [b] - [a+b]$. Define the *Stickelberger element of level l* in the rational group ring by

$$\theta(l) = \sum_{c \in \mathbf{F}_l^*} \left\langle \frac{c}{l} \right\rangle \sigma_c^{-1}.$$

Then for $ab(a+b) \not\equiv 0 \bmod l$ we have the following factorization of the Jacobi sum:

$$(J(\chi^a, \chi^b)) = P^{\Delta[a,b]\theta(l)},$$

where

$$\Delta[a, b]\theta(l) = \sum_{c \in \mathbf{F}_l^*} \left(\left\langle \frac{ac}{l} \right\rangle + \left\langle \frac{bc}{l} \right\rangle - \left\langle \frac{(a+b)c}{l} \right\rangle \right) \sigma_c^{-1}$$

lies in the integral group ring $\mathbf{Z}[G]$. Indeed, since

$$J(\chi^a, \chi^b)\overline{J}(\chi^a, \chi^b) = p$$

for any a, b with $ab(a+b) \not\equiv 0 \bmod l$, we see that of the $2m$ primes over (p), exactly m divide $J(\chi^a, \chi^b)$, and the conjugates of these divide $\overline{J}(\chi^a, \chi^b)$. So

$$\Delta[a, b]\theta(l) = \sum_{i=1}^{m} \sigma_{c_i}^{-1}, \qquad \sigma_{c_i} \neq \bar{\sigma}_{c_j}.$$

Let C be the Fermat curve defined by $X^l + Y^l + Z^l = 0$ over $\mathbf{F}_p$. Then by Weil [26] (or see [11, p. 22]), the zeta function $Z(C, T)$ is given by

$$Z(C, T) = \frac{\prod(1 - \alpha_{a,b}T)}{(1-T)(1-pT)},$$

where

$$\alpha_{a,b} = \chi^{(a+b)}(-1)J(\chi^a, \chi^b)$$

and the product ranges over $a, b \in \mathbf{F}_l$ with $ab(a+b) \not\equiv 0 \bmod l$.

Method. We will try to write a prime ideal P in $\mathbf{Z}[\zeta_l]$ over (p) as $P = (J_1, \ldots, J_m)$ for certain Jacobi sums $J_1, \ldots, J_m$. This method succeeds if and only if the Jacobi sums *separate* the primes, meaning, if P_i, P_j are distinct primes over (p), then there is a choice of a, b with $ab(a+b) \not\equiv 0 \bmod l$ such that

$$P_i \mid (J(\chi^a, \chi^b)) \quad \text{and} \quad P_j \nmid (J(\chi^a, \chi^b)).$$

The next three propositions show that the Jacobi sums do separate the prime ideals over (p). Indeed, there is a choice of (a, b) with the property that $J(\chi^a, \chi^b)$ and its conjugates under the Galois action separate the primes over (p).

Proposition 5.1. *Suppose that the Jacobi sums $J(\chi^a, \chi^b)$ do not separate the primes over (p). Then for each a, b*

$$\Delta[a, b]\theta(l) = \sum_{i=1}^{m} \sigma_{c_i}^{-1},$$

where $\{c_i : i = 1, \ldots, g\}$ is a union of cosets of a multiplicative subgroup of $\mathbf{F}_l^*$, other than the trivial subgroup, $\{1\}$.

Proof. Suppose P_i, P_j are not separated. Let a, b be integers with $ab(a+b) \not\equiv 0 \bmod l$. Suppose $\sigma_{e^n} P_i = P_j$, $n \neq 0$, where e is a generator of $\mathbf{F}_l^*$. Now suppose that σ_d is a summand in $\Delta[a, b]\theta(l)$. So $\sigma_d P \mid (J(\chi^a, \chi^b))$. Choose k so that $\sigma_k \sigma_d P = P_i$. Then

$$P_i \mid (\sigma_k J(\chi^a, \chi^b)), \qquad \sigma_k J(\chi^a, \chi^b) = J(\chi^{ka}, \chi^{kb}).$$

Since P_i, P_j are not separated, $P_j \mid (\sigma_k J(\chi^a, \chi^b))$ or, equivalently,

$$\sigma_k^{-1} \sigma_{e^n} \sigma_k \sigma_d P \mid (J(\chi^a, \chi^b)).$$

But $\sigma_k^{-1} \sigma_{e^n} \sigma_k \sigma_d = \sigma_{e^n} \sigma_d = \sigma_{e^n d}$. So $\sigma_{e^n d}$ is a summand in $\Delta[a, b]\theta(l)$. Thus, $\Delta[a, b]\theta(l) = \sum \sigma_{c_i}^{-1}$, where $\{c_i\}$ is a union of cosets of the multiplicative subgroup of $\mathbf{F}_l^*$ generated by e^n, which is nontrivial since $P_i \neq P_j$. □

Proposition 5.2. *Suppose that $\{c_i : i = 1, \ldots, m\}$ is a union of cosets of a nontrivial multiplicative subgroup of $\mathbf{F}_l^*$. Then $\sum_{i=1}^m c_i^{-1} = 0$ in $\mathbf{F}_l$.*

Proof. Let the subgroup be H, generated by $x \neq 1$, with $x^m = 1$, $|H| = m$. Let $a_1, \ldots, a_k$ be coset representatives. Then

$$\sum_{i=1}^{m} c_i^{-1} = \sum_{i=1}^{k} \sum_{n=0}^{m-1} (a_i x^n)^{-1} = \sum_{i=1}^{k} a_i^{-1} \sum_{n=0}^{m-1} x^n$$

$$= \sum_{i=1}^{k} a_i^{-1} \frac{x^m - 1}{x - 1} = 0. \quad \square$$

Proposition 5.3 [2, p. 183]. *Let l be an odd prime. There exist $a, b \in \mathbf{Z}$ with $ab(a+b) \not\equiv 0 \bmod l$ and*

$$\sum_{u \in \mathbf{F}_l^*} \left(- \left\langle \frac{(a+b)u}{l} \right\rangle + \left\langle \frac{au}{l} \right\rangle + \left\langle \frac{bu}{l} \right\rangle \right) u^{-1} \not\equiv 0 \mod l.$$

Proof. This proof is from [2], and uses the greater integer, [ ], rather than the fractional part $\langle\ \rangle$. Since $[x] + \langle x \rangle = x$ and $(a+b)u/l - au/l - bu/l = 0$,

$$\left\langle \frac{au}{l} \right\rangle + \left\langle \frac{bu}{l} \right\rangle - \left\langle \frac{(a+b)u}{l} \right\rangle = \left[\frac{(a+b)u}{l} \right] - \left[\frac{au}{l} \right] - \left[\frac{bu}{l} \right].$$

For $1 \leq u \leq l-1$, $[u/l] = 0$ and $[(l-1)u/l] = u - 1$. So

$$\sum_{m=1}^{l-2} \sum_{u=1}^{l-1} \left(\left[\frac{(m+1)u}{l} \right] - \left[\frac{mu}{l} \right] \right) u^{-1}$$

$$= \sum_{u=1}^{l-1} \left[\frac{l-1}{l} u \right] u^{-1} = \sum_{u=1}^{l-1} (u-1) u^{-1}$$

$$\equiv l - 1 \not\equiv 0 \bmod l.$$

So there is a pair $(a, b) = (m, 1)$, $m = 1, \ldots, l-2$, with the desired properties. $\square$

The algorithm. Let l, p be given with l an odd prime and $p \equiv 1 \bmod l$ also a prime. Construct the Jacobian variety J of the Fermat curve $X^l + Y^l + Z^l = 0$ over $\mathbf{Q}$, together with the addition law on it, following Chow [3]. Compute a bound B such that for $p \geq B$, the Fermat curve is smooth as a curve over $\mathbf{F}_p$, and the reduction of J and the group law on it modulo p gives the Jacobian of the Fermat curve as a curve over $\mathbf{F}_p$, and a group law on it.

We can assume that $p \geq B$. Reduce J mod p and compute the characteristic polynomial $P(t)$ of Frobenius in time polynomial in $\log p$, using the algorithm of Theorem A. Factor $P(t)$ over $\mathbf{Z}[\zeta_l]$. This can be done in time polynomial in the degree of $P(t)$ and the logarithms of the coefficients using A. K. Lenstra's extension to number fields [13] of the polynomial-time algorithm for factoring polynomials over $\mathbf{Q}$ due to A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász [14].

The roots $\{\alpha_1, \ldots, \alpha_{(l-1)(l-2)}\}$ of $P(t)$ are, up to units, the Jacobi sums $J(\chi^a, \chi^b)$ for $ab(a+b) \not\equiv 0 \bmod l$. By Propositions 5.1, 5.2, and 5.3, at

least one of these α_i has the property that it, and its conjugates, separate the prime ideals over (p). We therefore conclude with an exhaustive search, over all m element subsets of the G orbits of each α_i. The number of choices depends only on l, and a correct choice can be verified by trying to construct the corresponding root in $\mathbf{F}_p$.

Acknowledgments

This paper contains the results of the author's doctoral dissertation. It is a pleasure to thank my advisor, Peter Sarnak, for all his advice, help, and encouragement. I am indebted to H. W. Lenstra, Jr. for several very helpful comments and suggestions, particularly regarding §5. I have also benefited from conversations with R. Liviné, A. Clivio, and E. Kaltofen. I would like also to thank the referee for pointing out several inaccuracies and obscurities in a previous version of this paper. The work was partly supported by the NSF, grant number DMS 8610730.

Bibliography

1. L. M. Adleman and M.-D. Huang, *Recognizing primes in random polynomial time*, preprint, 1988.
2. L. M. Adleman, C. Pomerance, and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), 173–206.
3. W.-L. Chow, *The Jacobian variety of an algebraic curve*, Amer. J. Math. **76** (1954), 453–476.
4. S. Goldwasser and J. Kilian, *Almost all primes can be quickly certified*, Proc. 18th ACM Sympos. Theory of Computing, ACM, New York, 1986, pp. 316–329.
5. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford Univ. Press, Oxford, 1979.
6. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977.
7. G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788.
8. D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534.
9. M.-D. Huang, *Factorization of polynomials over finite fields and factorization of primes in algebraic number fields*, Proc. 16th ACM Sympos. Theory of Computing, ACM, New York, 1984, pp. 175–182.
10. ——, *Riemann hypothesis and finding roots over finite fields*, Proc. 17th ACM Sympos. Theory of Computing, ACM, New York, 1985, pp. 121–130.
11. S. Lang, *Cyclotomic fields*. I, Springer-Verlag, New York, 1978.
12. ——, *Abelian varieties*, Springer-Verlag, New York, 1983.
13. A. K. Lenstra, *Factoring polynomials over algebraic number fields*, Ph.D. thesis, Amsterdam, 1984.
14. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
15. E. W. Mayr and A. R. Meyer, *The complexity of the word problem for commutative semigroups and polynomial ideals*, Adv. in Math. **46** (1982), 305–329.
16. J. S. Milne, *Abelian varieties and Jacobian varieties*, Arithmetic Geometry, Chaps. V and VII (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, New York, 1986.
17. D. Mumford, *Abelian varieties*, 2nd ed., Oxford, 1974.

18. J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.
19. R. Schoof, *Elliptic curves over finite fields and the computation of square roots* mod p, Math. Comp. **44** (1985), 483–494.
20. A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.
21. I. R. Shafarevich, *Basic algebraic geometry*, Springer-Verlag, New York, 1977.
22. J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
23. B. L. van der Waerden, *Algebra*. II, Ungar, New York, 1970.
24. A. Weil, *Sur les courbes algébriques et les variétés qui s'en deduisent*, Hermann, Paris, 1948.
25. ____, *Variétés Abéliennes et courbes algébriques*, Hermann, Paris, 1948.
26. ____, *Jacobi sums as "Grössencharaktere"*, Trans. Amer. Math. Soc. **73** (1952), 487–495.
27. ____, *Foundations of algebraic geometry*, Colloq. Publ., vol. 39, Amer. Math. Soc., Providence, R.I., 1946.

SCHOOL OF MATHEMATICS, THE INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540

Current address: Department of Mathematics, Columbia University, New York, New York 10027