ERIC BACH, JOACHIM VON ZUR GATHEN & HENDRIK W. LENSTRA, JR. (2001). Factoring Polynomials over Special Finite Fields. *Finite Fields and Their Applications* **7**, 5–28. URL https://dx.doi.org/10.1006/ffta.2000.0306.

Factoring polynomials over special finite fields

Eric Bach, Joachim von zur Gathen, Hendrik W. Lenstra, Jr.

To Chao Ko, for his 90th birthday

Abstract. We exhibit a deterministic algorithm for factoring polynomials in one variable over finite fields. It is efficient only if a positive integer k is known for which $\Phi_k(p)$ is built up from small prime factors; here Φ_k denotes the kth cyclotomic polynomial, and p is the characteristic of the field. In the case $k{=}1$, when $\Phi_k(p){=}p{-}1$, such an algorithm was known, and its analysis required the generalized Riemann hypothesis. Our algorithm depends on a similar, but weaker, assumption; specifically, the algorithm requires the availability of an irreducible polynomial of degree r over $\mathbf{Z}/p\mathbf{Z}$ for each prime number r for which $\Phi_k(p)$ has a prime factor l with $l{\equiv}1 \bmod r$. An auxiliary procedure is devoted to the construction of roots of unity by means of Gauss sums. We do not claim that our algorithm has any practical value.

Key words: finite field, algorithm, factoring polynomials, Gauss sum.

1991 Mathematics subject classification: 11T16, 11T24, 12Y05.

Acknowledgements. This research was supported by NSF grants DCR-92-08639 [EB] and DMS-92-24205 [HWL], by NSERC grant 3-650-126-40 and by Fundación Andes grant C-10246 [JvzG]. Part of the research was carried out while the second author was in the Department of Computer Science of the University of Toronto. The first author thanks the Information Technology Research Centre, Province of Ontario, for sponsoring a visit to the University of Toronto in 1988, during which a first version of this paper was written.

1. Introduction

We present a theoretical result on the deterministic complexity of factoring polynomials over large finite fields. Let p be a prime number, k a positive integer, and $q = p^k$. We denote by $\mathbf{F}_q$ a finite field of cardinality q, and by Φ_k the kth cyclotomic polynomial. Let $S(q)$ be the set of prime numbers dividing $\Phi_k(p)$, and $s(q)$ the largest element of $S(q)$, with $s(2) = 1$. We let $R(q) = \{r : r \text{ is prime, and } r \text{ divides } l-1 \text{ for some prime number } l \in S(q)\}$.

Theorem 1. *There is a deterministic algorithm that, for some positive real number c, has the following property: given a prime number p, positive integers n and k, explicit data for $\mathbf{F}_{p^n}$, a non-zero polynomial $f \in \mathbf{F}_{p^n}[X]$, and for each prime number $r \in R(p^k)$ that does not divide n an irreducible polynomial g_r of degree r in $\mathbf{F}_p[X]$, the algorithm finds in time at most $(s(p^k) + \deg f + n \log p)^c$ the factorization of f into irreducible factors in $\mathbf{F}_{p^n}[X]$.*

The number k in Theorem 1 has no relation to n or f, and its role is purely auxiliary. It enters the run time estimate only through the number $s(p^k)$, which by (6.1) is at least $k/2$. For the definition of *explicit data* we refer to [12]. Time is measured in bit operations.

Elements of explicitly given finite fields—such as the coefficients of f and its factors, in Theorem 1—are required to be represented in the given model. Our proof of Theorem 1 is not merely existential, but allows for the effective construction of an algorithm with the listed properties.

Corollary. *There is a deterministic polynomial-time algorithm that factors polynomials in one variable over finite fields whose characteristic is a Fermat prime or a Mersenne prime.*

To deduce this from Theorem 1, we take $k = 1$ if $p = 2^m + 1$ is a Fermat prime and $k = 2$ if $p = 2^m - 1$ is a Mersenne prime; then we have $\Phi_k(p) = p \mp 1 = 2^m$ and $S(p^k) = \{2\}$, so that $R(p^k)$ is empty, and the result follows.

Generally, Theorem 1 establishes a relation between the deterministic complexity of the following two problems. The first is the problem of constructing an irreducible polynomial of given degree over a given finite field. The second is the problem of factoring polynomials over finite fields. V. Shoup [18] has shown that there is a deterministic polynomial-time "Turing" reduction of the first problem to the second. Theorem 1 shows that there is a similar reduction of the second problem to the first, provided that the characteristic p of the finite field has a special property; namely, a positive integer k should be available for which $\Phi_k(p)$ is built up from small prime factors. The same condition has been encountered in different circumstances (see [4; 13]), and not much is known about the distribution of prime numbers p for which a suitable k exists. The data of C. Pomerance and J. Sorenson [15] suggest that for large p and $k = 1$ or 2, the number $\Phi_k(p)$ is built up from small prime factors with roughly the same probability as a random number of the same size.

If the generalized Riemann hypothesis (GRH) is true, then Theorem 1 remains true even if the polynomials g_r are not given, since these can in that case be constructed by a deterministic polynomial-time algorithm [1]. Thus, Theorem 1 adds to the long list of special cases in which factoring polynomials over finite fields can be done deterministically in polynomial time, if GRH is granted; see [5, Notes on 7.8].

The case $k = 1$ of our result, with the g_r replaced by the assumption of GRH, was obtained by the second author [8] and independently by M. Mignotte and C. Schnorr [14]. Their method makes use of an $\mathbf{F}_p$-algebra all of whose units have order dividing $\Phi_1(p) = p - 1$, and those units are controlled by the availability—guaranteed through GRH—of "lth power non-residues" in $\mathbf{F}_p$, for each prime number l dividing $p - 1$. In extending this method to a proof of Theorem 1 one encounters several problems. The first is that one now

needs to construct, for general k, a sufficient supply of units of order dividing $\Phi_k(p)$, in some algebra over $\mathbf{F}_p$. We solve this problem by means of a pretty formula, which is given in Proposition (5.2). Secondly, there is the problem of constructing the analogues of lth power non-residues. The natural way of doing this (cf. [9]) would require an irreducible rth degree polynomial $g_r \in \mathbf{F}_p[X]$ to be known for each prime number r dividing the product $\prod_{m\geq 0} \varphi^m(\Phi_k(p))$, where φ^m denotes the mth iterate of the Euler φ-function; this includes the primes in $R(p^k)$, which all divide $\varphi(\Phi_k(p))$. The fact that Theorem 1 economizes on the g_r, and requires them only for $r \in R(p^k)$, makes the construction somewhat laborious. Two auxiliary results that we need in this context can be formulated as follows.

Theorem 2. *There is a deterministic algorithm that, for some positive real number c, has the following property: given two prime numbers p and l, a positive integer h for which $p^h \equiv 1 \bmod l$, explicit data for $\mathbf{F}_{p^h}$, and, for each prime number r dividing $l-1$ but not dividing h, an irreducible polynomial g_r of degree r in $\mathbf{F}_p[X]$, the algorithm constructs in time at most $(l + h\log p)^c$ a primitive lth root of unity in $\mathbf{F}_{p^h}$.*

The proof of Theorem 2 makes use of Gauss sums in a certain algebra over $\mathbf{F}_{p^h}$.

Theorem 3. *There is a deterministic algorithm that, for some positive real number c, has the following property: given a prime number p, a positive integer k, explicit data for $\mathbf{F}_{p^k}$, and, for each $l \in S(p^k)$, a primitive lth root of unity in $\mathbf{F}_{p^k}$, the algorithm constructs, in time at most $(s(p^k) + k\log p)^c$, for each $l \in S(p^k)$ an element of $\mathbf{F}_{p^k}$ that is not an lth power in $\mathbf{F}_{p^k}$.*

The case $k = 1$ of Theorem 3 is due to L. Rónyai [16]. Our proof of the general case depends, again, on our method of constructing elements of order dividing $\Phi_k(p)$ in certain algebras.

In Section 2 we assemble a few theoretical and algorithmic results about roots of unity in rings. Section 3 is devoted to Gauss sums and Jacobi sums. In Sections 4, 5, and 6 we prove Theorems 2, 3, and 1, respectively.

At several points in the paper we shall refer to *Berlekamp's algorithm*. By this we shall always mean an algorithm that factors any non-zero f in $\mathbf{F}_q[X]$ in time $(p + \deg f + \log q)^{O(1)}$, see [6; 5, Exercise 7.17]. Berlekamp's algorithm shows that Theorem 1 is of interest only for "large" p.

Whenever we assert that an algorithm with certain properties exists, such an algorithm is actually exhibited, explicitly or implicitly, in the paper itself or in the papers that we

refer to. Any algorithmic choices and recommendations that we make are inspired by the desire to give a valid and quick proof of our results, and no effort has been made to optimize the efficiency of the algorithms; in fact, we would be surprised if our results had any implication for the practical problem of factoring polynomials over finite fields.

Rings are supposed to be commutative with 1, and the unit element is supposed to be preserved by ring homomorphisms. The group of units of a ring R is denoted by R^*, and for $u \in R^*$ we write $\langle u \rangle$ for the subgroup of R^* generated by u. If K is a field, a *K-algebra* is a ring R equipped with a ring homomorphism $K \to R$.

2. Strict roots of unity

Let R be a ring. If n is a positive integer, then we call an element $\zeta \in R$ a *strict nth root of unity* if $\zeta^n = 1$ and $\zeta^{n/r} - 1 \in R^*$ for each prime number r dividing n. Obviously, if R is a field, then a strict nth root of unity is the same as a primitive nth root of unity.

Proposition (2.1). *Suppose that $\zeta \in R$ is a strict nth root of unity. Then we have:*

(a) *if R is non-zero, then ζ has multiplicative order n;*

(b) *if $f\colon R \to R'$ is a ring homomorphism, then $f(\zeta)$ is a strict nth root of unity in R';*

(c) *$\zeta^i - \zeta^j \in R^*$ whenever i, j are integers with $i \not\equiv j \bmod n$;*

(d) *$\prod_{i=0}^{n-1}(X - \zeta^i) = X^n - 1$ in the polynomial ring $R[X]$;*

(e) *if n' is a positive integer all of whose prime factors divide n, and $\epsilon \in R$ satisfies $\epsilon^{n'} = \zeta$, then ϵ is a strict $n'n$th root of unity;*

(f) *if n' is a positive integer with $\gcd(n', n) = 1$, and $\epsilon \in R$ is a strict n'th root of unity, then $\epsilon\zeta$ is a strict $n'n$th root of unity;*

(g) *ζ^i is a strict $n/\gcd(n, i)$th root of unity for each integer i;*

(h) *if $\nu \subset \langle \zeta \rangle$ is any subgroup of order greater than 1, then $\sum_{\epsilon \in \nu} \epsilon = 0$.*

Proof. Parts (a) and (b) are obvious.

(c) The image $\bar{\zeta}$ of ζ in the ring $\bar{R} = R/(\zeta^i - \zeta^j)R$ satisfies $\bar{\zeta}^i = \bar{\zeta}^j$ and has therefore order less than n. By (b), it is a strict nth root of unity, so (a) implies that $\bar{R}$ is the zero ring. Therefore we have $\zeta^i - \zeta^j \in R^*$.

(d) If R is a field, and a polynomial $f \in R[X]$ has pairwise distinct zeroes $a_i \in R$, then f is divisible by $\prod_i (X - a_i)$ (see [10, Chapter IV, Theorem 1.4 and proof]). The same proof shows that this remains true if R is a ring and $a_i - a_j \in R^*$ for all $i \neq j$. Applying this to $f = X^n - 1$ and $a_i = \zeta^i$ one obtains (d).

Part (e) is immediate from the definition, and (f) and (g) are easy consequences of (c).

(h) Let $\eta \in \nu$, $\eta \neq 1$. We have $\eta\nu = \nu$, so the sum $\sum_{\epsilon\in\nu} \epsilon$ is unchanged under multiplication by η, and therefore annihilated by $\eta - 1$. Since the latter element is a unit, this implies that the sum vanishes.

This proves (2.1).

Proposition (2.2). *Let $\zeta \in R$, and let n be a positive integer. Then ζ is a strict nth root of unity in R if and only if $\Phi_n(\zeta) = 0$ and $n \cdot 1 \in R^*$.*

Proof. "If". Suppose that $\Phi_n(\zeta) = 0$ and $n \cdot 1 \in R^*$. Since Φ_n divides $X^n - 1$ in $\mathbf{Z}[X]$ we have $\zeta^n = 1$. Next let r be a prime number dividing n. Since Φ_n divides the polynomial $(X^n - 1)/(X^{n/r} - 1) = \sum_{i=0}^{r-1} X^{in/r}$, we have $\sum_{i=0}^{r-1} \zeta^{in/r} = 0$. Take this modulo $\zeta^{n/r} - 1$; by $\zeta^{in/r} \equiv 1 \bmod (\zeta^{n/r} - 1)$ this gives $r \cdot 1 \equiv 0 \bmod (\zeta^{n/r} - 1)$, and therefore $n \cdot 1 \equiv 0 \bmod (\zeta^{n/r} - 1)$. Since $n \cdot 1$ is a unit, this implies that $\zeta^{n/r} - 1$ is a unit as well.

"Only if". Suppose that ζ is a strict nth root of unity in R. Since $X^n - 1$ divides $\Phi_n \cdot \prod_r (X^{n/r} - 1)$, the product ranging over the primes r dividing n, we have $\Phi_n(\zeta) \cdot \prod_r (\zeta^{n/r} - 1) = 0$. The factors $\zeta^{n/r} - 1$ are units, so it follows that $\Phi_n(\zeta) = 0$. Dividing the identity in (2.1)(d) by $X - 1$ (which is not a zero-divisor in $R[X]$) and substituting 1 for X we find that $\prod_{i=1}^{n-1}(1 - \zeta^i) = n \cdot 1$. By (2.1)(c), this shows that $n \cdot 1 \in R^*$. This proves (2.2).

An element $e \in R$ is called an *idempotent* if $e^2 = e$. An idempotent e is said to be *trivial* if $e = 0$ or $e = 1$.

Proposition (2.3). *Suppose that $\zeta \in R$ is a strict nth root of unity, and that $\alpha \in R$ satisfies $\alpha^n = 1$. Then there is a non-trivial idempotent in R or there exists i (mod n) with $\alpha = \zeta^i$.*

Proof. Substituting α for X in the identity from (2.1)(d) we find that $\prod_{i=0}^{n-1}(\alpha - \zeta^i) = 0$. Hence, if we put $I_i = (\alpha - \zeta^i)R$, then the product of the ideals I_i is zero. Also, the I_i are pairwise coprime, since $I_i + I_j$ contains the element $-(\alpha - \zeta^i) + (\alpha - \zeta^j) = \zeta^i - \zeta^j$, which by (2.1)(c) is a unit if $i \neq j$. The Chinese remainder theorem [3, Proposition 1.10] now implies that the natural map $R \to \prod_{i=0}^{n-1} R/I_i$ is an isomorphism. If at least two of the rings R/I_i are non-zero—one of which is R/I_h, say—then the unique element $e \in R$ that is congruent to 1 modulo I_h and to 0 modulo all other I_i is a non-trivial idempotent. If at most one of the rings R/I_i is non-zero, then all but at most one of the $\alpha - \zeta^i$ are units; in that case the $\alpha - \zeta^i$ that was excluded is zero. This proves (2.3).

Proposition (2.4). *Let m and n be positive integers, and let α, $\gamma \in R$. Suppose that $\alpha^m = 1$ and that γ^m is a strict nth root of unity. Then there exists $\beta \in R^*$ with $\beta^n = \alpha$.*

Proof. Write $m = m'n'$, where m' is the largest divisor of m that is coprime to n. Then each prime dividing n' divides n, so (2.1)(e) implies that $\gamma^{m'}$ is a strict $n'n$th root of unity and (2.1)(g) that $\gamma^{m'n}$ is a strict n'th root of unity. By (2.1)(d) we have $\prod_{i=0}^{n'-1}(X - \gamma^{im'n}) = X^{n'} - 1$. Substituting $\alpha^{m'}$ for X we find that $\prod_{i=0}^{n'-1}(\alpha^{m'} - \gamma^{im'n}) = 0$. Thus, if we now put $I_i = (\alpha^{m'} - \gamma^{im'n})R$, then as in the proof of (2.3) we deduce that the natural map $R \to \prod_{i=0}^{n'-1} R/I_i$ is an isomorphism. Let δ be the element of R that maps to $(\gamma^{im'})_i \in \prod_{i=0}^{n'-1} R/I_i$. Since $\alpha^{m'} \equiv \gamma^{im'n} \bmod I_i$ it follows that $\alpha^{m'} = \delta^n$. To finish the proof, let u, v be integers satisfying $um' + vn = 1$, and put $\beta = \delta^u \alpha^v$; then we have $\beta^n = \delta^{un}\alpha^{vn} = \alpha^{um'+vn} = \alpha$, as required. This proves (2.4).

The proofs of (2.3) and (2.4) provide fairly explicit constructions of the elements that are asserted to exist. However, for algorithmic purposes the product over all n or n' values of i may be too large. Thus, in the algorithmic versions of (2.3) and (2.4) that follow, we replace n and n' by a prime factor, and we proceed recursively.

Let p be a prime number, and let R be an $\mathbf{F}_p$-algebra of finite vector space dimension d over $\mathbf{F}_p$; then the order of R equals p^d. By *explicit data* for R we mean a system $(a_{hij})_{1 \le h,i,j \le d}$ of d^3 elements of $\mathbf{F}_p$ such that for some vector space basis $(e_i)_{i=1}^d$ of R over $\mathbf{F}_p$ one has $e_h e_i = \sum_j a_{hij} e_j$ for all h, i; when R is given by means of explicit data, then elements of R are supposed to be specified by means of their coefficients on the same basis, these coefficients as well as the a_{hij} being represented as integers modulo p in the conventional way (cf. [12, Section 2; 7, Section 2]).

Proposition (2.5). *There is a deterministic algorithm that, for some positive real number c, has the following property: given a prime number p, explicit data for a non-zero $\mathbf{F}_p$-algebra R of order p^d, an integer $n > 1$, and elements α, $\zeta \in R$ as in* (2.3)*, the algorithm computes in time at most $(s + d \log p)^c$ either a non-trivial idempotent $e \in R$ or an integer $i \pmod n$ with $\alpha = \zeta^i$; here s denotes the largest prime factor of n.*

Proof. The algorithm begins by factoring n completely, which can be done in time $(s + \log n)^{O(1)}$; note that, since R contains a strict nth root of unity, we have $n < \#R$ and therefore $\log n < d \log p$. Once n is factored, one proceeds in the following recursive fashion, replacing n by a proper divisor in every step.

If $n = 1$ then one can clearly take $i = 0$. Suppose now that $n > 1$, and let r be a

prime factor of n. As in the proof of (2.3), with $\alpha^{n/r}$, $\zeta^{n/r}$, and r in the roles of α, ζ, and n, one has $\prod_{i=0}^{r-1}(\alpha^{n/r} - \zeta^{in/r}) = 0$. With $I_i = (\alpha^{n/r} - \zeta^{in/r})R$, the natural map $R \to \prod_{i=0}^{r-1} R/I_i$ is an isomorphism. Using linear algebra over $\mathbf{F}_p$ one determines which of the elements $\alpha^{n/r} - \zeta^{in/r}$ are non-units or, equivalently, which of the rings R/I_i are non-zero. This occurs for at least one of the rings, say for R/I_h. If it occurs for at least one other ring R/I_i, then one uses linear algebra to determine the unique element $e \in R$ with $e \equiv 1 \bmod I_h$ and $e \equiv 0 \bmod I_i$ for all $i \neq h$; this is a non-trivial idempotent, and the algorithm stops in this case. If R/I_h is the only non-zero ring among the R/I_i, then one has actually $R = R/I_h$, so $I_h = \{0\}$ and $\alpha^{n/r} = \zeta^{hn/r}$. In this case one calls the algorithm recursively on $\alpha\zeta^{-h}$, ζ^r, and n/r in the roles of α, ζ, and n. Then one obtains either a non-trivial idempotent e in R or an integer $j \pmod{n/r}$ with $\alpha\zeta^{-h} = \zeta^{jr}$; in the latter case one computes $i = jr + h$, which does satisfy $\alpha = \zeta^i$, and the algorithm stops.

It is clear that this algorithm has the stated properties. This proves (2.5).

Proposition (2.6). *There is a deterministic algorithm that, for some positive real number c, has the following property: given a prime number p, explicit data for a non-zero $\mathbf{F}_p$-algebra R of order p^d, integers $m > 0$ and $n > 1$, and elements α, $\gamma \in R$ as in* (2.4)*, the algorithm computes in time at most $(s + \log m + d \log p)^c$ an element $\beta \in R^*$ with $\beta^n = \alpha$; here s denotes the largest prime factor of n.*

Proof. Again, one starts by factoring n completely. Next, one proceeds recursively, replacing m by a proper divisor in every step.

If m is divisible by none of the primes dividing n, then one computes v with $vn \equiv 1 \bmod m$, and one puts $\beta = \alpha^v$; we have indeed $\beta^n = \alpha$, since $\alpha^m = 1$. In the other case, let r be a prime factor of n that divides m. Then we have $\prod_{i=0}^{r-1}(\alpha^{m/r} - \gamma^{imn/r}) = 0$. With $I_i = (\alpha^{m/r} - \gamma^{imn/r})R$, the natural map $R \to \prod_{i=0}^{r-1} R/I_i$ is an isomorphism, so using linear algebra over $\mathbf{F}_p$ one can find the unique element $\delta \in R$ that for each $i = 0, 1, \ldots, r-1$ satisfies $\delta \equiv \gamma^i \bmod I_i$; then we have $\alpha^{m/r} = \delta^{nm/r}$, so for $\tilde{\alpha} = \alpha/\delta^n$ and $\tilde{m} = m/r$ we have $\tilde{\alpha}^{\tilde{m}} = 1$. Now one calls the algorithm recursively on $\tilde{\alpha}$, $\tilde{m}$, and $\tilde{\gamma} = \gamma^r$. Then one finds $\tilde{\beta} \in R$ with $\tilde{\beta}^n = \tilde{\alpha}$, and one puts $\beta = \tilde{\beta}\delta$.

Again, the verification that the algorithm just described has the asserted properties is completely straightforward. This proves (2.6).

The algorithm of (2.6) can, in substance, be found in [7, Proposition 7]. It can also be used for other rings that are sufficiently explicitly given (cf. [11, Section 2]).

3. Gauss sums

In this section we let K be a field.

(3.1) *The Teichmüller subgroup.* Let r be a prime number different from the characteristic of K. We write $K[\zeta_r]$ for the ring $K[X]/\left(\sum_{i=0}^{r-1} X^i\right)$, and we let ζ_r denote the residue class of X. For each $a \in \mathbf{F}_r^*$, the ring $K[\zeta_r]$ has a unique automorphism ρ_a that is the identity on K and satisfies $\rho_a \zeta_r = \zeta_r^a$. The set of all ρ_a's forms a group, which we denote by Δ_r; the map assigning ρ_a to a establishes a group isomorphism $\mathbf{F}_r^* \cong \Delta_r$, so Δ_r is cyclic with generator ρ_g, where g is a primitive root modulo r. Denote by $\mathbf{Z}_r$ the ring of r-adic integers, and define the *Teichmüller character* $\omega\colon \mathbf{F}_r^* \to \mathbf{Z}_r^*$ by $\omega(b \bmod r) = \lim_{k\to\infty} b^{r^k}$. Following [12, Section 4], we define the *Teichmüller subgroup* T_r of $K[\zeta_r]^*$ to be the set of those $\epsilon \in K[\zeta_r]^*$ that have r-power order and satisfy $\rho_a \epsilon = \epsilon^{\omega(a)}$ for all $a \in \mathbf{F}_r^*$. We have $\zeta_r \in T_r$.

Proposition (3.2). (a) *Every finite subgroup of T_r is cyclic.*

(b) *Every non-trivial subgroup of T_r contains ζ_r.*

(c) *Every $\epsilon \in T_r$ is a strict nth root of unity, for $n = \operatorname{order} \epsilon$.*

(d) *Suppose that K is finite, of order q, and let m_r be the multiplicative order of $(q \bmod r)$ in $\mathbf{F}_r^*$. Then each element of $K[\zeta_r]^*$ has order dividing $q^{m_r} - 1$, and T_r is cyclic of order equal to the largest power of r dividing $q^{m_r} - 1$.*

Proof. For (a), see [12, (4.2)]. Every non-trivial subgroup of T_r has a subgroup of order r, and since T_r has at most one subgroup of order r, by (a), it must be $\langle \zeta_r \rangle$. This proves (b). From (2.2) it follows that ζ_r is a strict rth root of unity. By (2.1)(g), the other elements of $\langle \zeta_r \rangle$ are strict roots of unity as well, and by (b) and (2.1)(e) the same is true for all $\epsilon \in T_r$. This proves (c). If K is finite of order q, then the ring homomorphism from $K[\zeta_r]$ to itself that raises each element to the power q^{m_r} is the identity both on K and on $\langle \zeta_r \rangle$, so it is the identity; hence each $u \in K[\zeta_r]^*$ has order dividing $q^{m_r} - 1$. The last assertion of (d) is in [12, (5.1)]. This proves (3.2).

The following technical lemma will be needed later.

Lemma (3.3). *Let g be a primitive root modulo r. Then the element*

$$\alpha = (1 - r)^{-1} \cdot \sum_{i=1}^{r-2} i\omega(g)^i \rho_g^{-i-1}$$

of the group ring $\mathbf{Z}_r[\Delta_r]$ *satisfies* $\alpha \cdot (\rho_g - \omega(g))^2 = \rho_g - \omega(g)$.

Remark. This lemma expresses in an explicit manner the existence of an idempotent $\alpha \cdot (\rho_g - \omega(g))$ in $\mathbf{Z}_r[\Delta_r]$ that generates the kernel of the ring homomorphism $\mathbf{Z}_r[\Delta_r] \to \mathbf{Z}_r$ induced by ω.

Proof. The element $\omega(g) \in \mathbf{Z}_r$ is a zero of the polynomial $f_0 = X^{r-1} - 1$, and if we write $f_0 = f_1 \cdot (X - \omega(g))$ then we have $f_1(\omega(g)) = f_0'(\omega(g)) = (r-1)\omega(g)^{r-2} = (r-1)\omega(g)^{-1}$. Hence we can perform a division with remainder $(*)$ $f_1 = f_2 \cdot (X - \omega(g)) + (r-1)\omega(g)^{-1}$, and an explicit long division shows that $f_2 = \sum_{i=1}^{r-2} i\omega(g)^{i-1} X^{r-2-i}$. Multiplying $(*)$ by $(1-r)^{-1} \cdot \omega(g) \cdot (X - \omega(g))$ we find that

$$(1-r)^{-1} \cdot \omega(g) \cdot f_2 \cdot (X - \omega(g))^2 \equiv X - \omega(g) \bmod (X^{r-1} - 1).$$

Substituting ρ_g for X we obtain the lemma.

(3.4) *A larger ring.* In the rest of this section, we let l be a prime number, and we suppose that K contains a primitive lth root of unity η; then it contains $l-1$ of them. We make the further assumptions that $l-1$ is not divisible by the characteristic of K, and that for each prime number r dividing $l-1$ the group T_r contains a subgroup of order equal to the largest power of r dividing $l-1$; we write $\mu_{(r)}$ for this subgroup. By (3.2)(c), all elements of $\mu_{(r)}$ are strict roots of unity.

We write A for the tensor product, over K, of the rings $K[\zeta_r]$, with r ranging over the primes dividing $l-1$; explicitly, if these primes are $r_1, \ldots, r_t$ (without repetition), then A is the ring $K[X_1, \ldots, X_t] / \left(\sum_{i=0}^{r_1-1} X_1^i, \ldots, \sum_{i=0}^{r_t-1} X_t^i\right)$; as a vector space over K, it has dimension $\prod_{i=1}^{t}(r_i - 1)$. Each of the rings $K[\zeta_r]$ embeds in a natural way in A. The groups $\mu_{(r)}$ generate a subgroup of A^*, which we denote by μ; it is cyclic of order $l-1$, and it is, by (2.1)(f), generated by a strict $(l-1)$th root of unity. Thus from (2.1)(h) we obtain

$$\sum_{\epsilon \in \nu} \epsilon = 0 \qquad \text{for each subgroup } \nu \neq \{1\} \text{ of } \mu, \tag{3.5}$$

a fact that will be used repeatedly below.

(3.6) *Jacobi sums and Gauss sums.* We denote by Ψ the group of group homomorphisms $\mathbf{F}_l^* \to \mu$; then Ψ is cyclic of order $l-1$. We denote the unit element of Ψ simply by 1. For χ, $\psi \in \Psi$, we define the *Jacobi sum* $j(\chi, \psi) \in A$ by

$$j(\chi, \psi) = \begin{cases} -\sum_{x,y \in \mathbf{F}_l^*, x+y=1} \chi(x)\psi(y) & \text{if } \chi \neq 1,\ \psi \neq 1,\ \chi\psi \neq 1, \\ \chi(-1) \cdot l & \text{if } \chi \neq 1,\ \chi\psi = 1, \\ 1 & \text{if } \chi = 1 \text{ or } \psi = 1. \end{cases}$$

For $\chi \in \Psi$ and a primitive lth root of unity $\eta \in K$, we define the *Gauss sum* $\tau(\chi, \eta) \in A$ by

$$\tau(\chi, \eta) = -\sum_{x \in \mathbf{F}_l^*} \chi(x)\eta^x.$$

We list the basic properties of these sums that we shall need.

Proposition (3.7). *Let $\eta \in K$ be a primitive lth root of unity. Then we have:*

(a) $\tau(1, \eta) = 1$;

(b) $\tau(\chi, \eta)\tau(\psi, \eta) = j(\chi, \psi)\tau(\chi\psi, \eta)$ *for all* χ, $\psi \in \Psi$;

(c) $j(\chi, \psi) \in A^*$, $\tau(\chi, \eta) \in A^*$ *for all* χ, $\psi \in \Psi$;

(d) $\eta = (1 - l)^{-1} \sum_{\chi \in \Psi} \tau(\chi, \eta)$;

(e) $\tau(\chi, \eta^y) = \chi(y)^{-1}\tau(\chi, \eta)$ *for all* $\chi \in \Psi$ *and* $y \in \mathbf{F}_l^*$;

(f) *if r is a prime dividing $l - 1$, and $\chi \in \Psi$ has r-power order, then $\tau(\chi, \eta)$ belongs to the subring $K[\zeta_r]$ of A, and one has $\rho_a(\tau(\chi, \eta)) = \tau(\chi^{\omega(a)}, \eta)$ for all $a \in \mathbf{F}_r^*$.*

Proof. (a) We have $\tau(1, \eta) = -\sum_{i=1}^{l-1} \eta^i = 1$.

(b) This is clear from (a) if $\chi = 1$ or $\psi = 1$. Next suppose that $\chi \neq 1$ and $\psi \neq 1$. We have

$$\tau(\chi, \eta)\tau(\psi, \eta) = \sum_{x,y \in \mathbf{F}_l^*} \chi(x)\psi(y)\eta^{x+y} = \sum_{z \in \mathbf{F}_l} \Big(\sum_{x,y \in \mathbf{F}_l^*, x+y=z} \chi(x)\psi(y) \Big) \eta^z$$

$$= \sum_{x,y \in \mathbf{F}_l^*, x+y=0} \chi(x)\psi(y) + \sum_{z \in \mathbf{F}_l^*} \Big(\sum_{x,y \in \mathbf{F}_l^*, x+y=1} \chi(xz)\psi(yz) \Big) \eta^z$$

$$= \chi(-1) \sum_{y \in \mathbf{F}_l^*} \chi\psi(y) - \Big(\sum_{x,y \in \mathbf{F}_l^*, x+y=1} \chi(x)\psi(y) \Big) \tau(\chi\psi, \eta).$$

If $\chi\psi \neq 1$ then from (3.5), with ν equal to the image of $\chi\psi$, we see that $\sum_{y \in \mathbf{F}_l^*} \chi\psi(y) = 0$. In that case we obtain (b), as required. If $\chi\psi = 1$, then we find that

$$\tau(\chi, \eta)\tau(\psi, \eta) = \chi(-1)(l - 1) - \Big(\sum_{x \in \mathbf{F}_l^*, x \neq 1} \chi(x/(1 - x)) \Big) \tau(1, \eta)$$

$$= \chi(-1)(l - 1) - \sum_{z \in \mathbf{F}_l^*, z \neq -1} \chi(z) = \chi(-1)(l - 1) + \chi(-1) = \chi(-1) \cdot l = j(\chi, \psi),$$

where we use that $\sum_{z \in \mathbf{F}_l^*} \chi(z) = 0$, which again follows from (3.5).

(c) Since l is not divisible by the characteristic of K, it is a unit in A, so $j(\chi, \psi) \in A^*$ whenever at least one of χ, ψ, and $\chi\psi$ equals 1. Applying (b) to $\psi = \chi^{-1}$ we now see, using (a), that $\tau(\chi, \eta) \in A^*$ for all χ. Next we see from (b) that $j(\chi, \psi) \in A^*$ for all χ, ψ.

(d) We have $\sum_{\chi\in\Psi}\tau(\chi,\eta)=\sum_{x\in\mathbf{F}_l^*}\big(-\sum_{\chi\in\Psi}\chi(x)\big)\eta^x$. By (3.5), the sum in parentheses vanishes for every $x\neq 1$, and we are left with the contribution for $x=1$, which is $(1-l)\eta$.

(e) We have $\chi(y)\tau(\chi,\eta^y)=-\sum_{x\in\mathbf{F}_l^*}\chi(yx)\eta^{yx}=\tau(\chi,\eta)$, using yx as a new summation variable.

(f) Under the hypotheses of (f), the image of χ is in $\mu_{(r)}$, so that $\tau(\chi,\eta)\in K[\zeta_r]$. The equality in (f) follows from the fact that ρ_a fixes the elements η^x of K and raises the elements $\chi(x)$ of T_r to the power $\omega(a)$.

This proves (3.7).

The following lemma will be our main tool in computing Gauss sums.

Lemma (3.8). *Let r be a prime number dividing $l-1$, let t be a non-negative integer, let g be a primitive root modulo r, and let G be a positive integer that is congruent to $\omega(g)$ modulo r^t. Suppose that $\chi\in\Psi$, $\chi\neq 1$, is of order r^t, and that $\upsilon\in K[\zeta_r]$ is such that $\upsilon^{r^t}=\tau(\chi,\eta)^{r^t}$ for some primitive lth root of unity $\eta\in K$. Define*

$$\epsilon=\frac{\upsilon^G}{\rho_g(\upsilon)}\cdot\frac{\tau(\chi^G,\eta)}{\tau(\chi,\eta)^G},\qquad \vartheta=\prod_{i=1}^{r-2}\rho_g^{-i-1}(\epsilon)^{iG^i(1-r^t)/(1-r)}.$$

Then there exists a primitive lth root of unity $\eta'\in K$ such that $\vartheta\cdot\upsilon=\tau(\chi,\eta')$.

Remark. The following may serve to explain what is happening in this lemma and its proof. If the r^tth root of unity δ with $\delta\upsilon=\tau(\chi,\eta)$ belongs to T_r—which occurs, for example, if $K[\zeta_r]$ is a field—then (3.7)(e) readily implies that υ itself is of the form $\tau(\chi,\eta')$; in this case, one has $\epsilon=1$ and $\vartheta=1$. In general, δ must be replaced by its projection δ/ϑ to T_r, which is to be computed with the help of the idempotent $\alpha\cdot\big(\rho_g-\omega(g)\big)$ from Lemma (3.3). However, since δ is just as unavailable as $\tau(\chi,\eta)$, the required computation cannot be done directly, and this necessitates the detour over ϵ.

Proof. The action of Δ_r on $K[\zeta_r]^*$ makes the latter group into a module over the group ring $\mathbf{Z}[\Delta_r]$. We write the action of this group ring exponentially. For example, in this notation we can rewrite the definition of ϵ as $\epsilon=\upsilon^{G-\rho_g}\cdot\tau(\chi,\eta)^{\rho_g-G}$ (applying (3.7)(f) to $a=g$).

From $\tau(\chi,\eta)\in K[\zeta_r]^*$ and $\upsilon^{r^t}=\tau(\chi,\eta)^{r^t}$ we find that $\delta\upsilon=\tau(\chi,\eta)$ for some $\delta\in K[\zeta_r]^*$ with $\delta^{r^t}=1$. Applying ρ_g-G we find that

$$\delta^{\rho_g-G}=\upsilon^{G-\rho_g}\cdot\tau(\chi,\eta)^{\rho_g-G}=\epsilon.$$

This shows that $\epsilon^{r^t} = 1$, so that both δ and ϵ belong to the group of elements of $K[\zeta_r]^*$ of r-power order. That group is a $\mathbf{Z}_r[\Delta_r]$-module. In the definition of ϑ, the exponent $iG^i(1-r^t)/(1-r)$ matters only modulo r^t, so we may rewrite that definition as $\vartheta = \epsilon^\alpha$, where $\alpha \in \mathbf{Z}_r[\Delta_r]$ is as in Lemma (3.3). Using (3.3) and applying $\alpha(\rho_g - \omega(g))$ to the equality $\delta^{\rho_g - \omega(g)} = \epsilon$ we now find that

$$\delta^{\rho_g - \omega(g)} = \delta^{\alpha(\rho_g - \omega(g))^2} = \epsilon^{\alpha(\rho_g - \omega(g))} = \vartheta^{\rho_g - \omega(g)}.$$

Therefore the element δ/ϑ, which has order dividing r^t, satisfies $\rho_g(\delta/\vartheta) = (\delta/\vartheta)^{\omega(g)}$. Since g generates $\mathbf{F}_r^*$ it follows, by the definition of T_r, that δ/ϑ belongs to T_r. In fact, it belongs to the image $\chi(\mathbf{F}_l^*)$ of χ; to prove this, it suffices to observe that T_r is cyclic and that the order of δ/ϑ divides the order r^t of the subgroup $\chi(\mathbf{F}_l^*)$ of T_r. Thus we can write $\delta/\vartheta = \chi(y)$, with $y \in \mathbf{F}_l^*$. Now we have

$$\vartheta \cdot \upsilon = (\vartheta/\delta) \cdot \tau(\chi, \eta) = \chi(y)^{-1}\tau(\chi, \eta) = \tau(\chi, \eta^y),$$

using (3.7)(e). This proves (3.8), with $\eta' = \eta^y$.

Lemma (3.9). *Let $\chi_1, \ldots, \chi_t \in \Psi$ be characters whose orders are pairwise relatively prime, and let $\eta_1, \ldots, \eta_t \in K$ be primitive lth roots of unity. Then there exists a primitive lth root of unity $\eta \in K$ such that for each $i = 1, \ldots, t$ one has $\tau(\chi_i, \eta) = \tau(\chi_i, \eta_i)$.*

Proof. We may assume that $t > 0$. Write $\eta_i = \eta_1^{z(i)}$ for each i, with $z(i) \in \mathbf{F}_l^*$ (and $z(1) = 1$). Since the orders of the χ_i are pairwise coprime, the Chinese remainder theorem implies that the map $\mathbf{F}_l^* \to \prod_{i=1}^t \chi_i(\mathbf{F}_l^*)$ sending y to $\big(\chi_i(y)\big)_{i=1}^t$ is surjective. Choose $y \in \mathbf{F}_l^*$ mapping to $\big(\chi_i(z(i))\big)_{i=1}^t$. By (3.7)(e), we have

$$\tau(\chi_i, \eta_1^y) = \chi_i(y)^{-1} \cdot \tau(\chi_i, \eta_1) = \chi_i(z(i))^{-1} \cdot \tau(\chi_i, \eta_1) = \tau(\chi_i, \eta_1^{z(i)}) = \tau(\chi_i, \eta_i)$$

for each $i = 1, \ldots, t$, which proves the lemma, with $\eta = \eta_1^y$.

4. Constructing roots of unity

In this section we describe the algorithm that proves Theorem 2.

We are given two prime numbers p and l, a positive integer h for which l divides p^h-1, explicit data for $\mathbf{F}_{p^h}$, and, for each prime number r dividing $l-1$ but not dividing h, an irreducible polynomial g_r of degree r in $\mathbf{F}_p[X]$. It is our purpose to construct a primitive lth root of unity in $\mathbf{F}_{p^h}$, in time $(l+h\log p)^{O(1)}$.

If p divides $l-1$, then it suffices to apply Berlekamp's algorithm (see Section 1) for finding a zero of $\sum_{i=0}^{l-1} X^i$ in $\mathbf{F}_{p^h}$. Each zero is a primitive lth root of unity. Note that Berlekamp's algorithm is fast enough for our purpose if p divides $l-1$. Let it henceforth be assumed that p does not divide $l-1$, and write

$$l-1=\prod_r r^{a(r)},$$

with r ranging over the prime numbers dividing $l-1$ and each $a(r)$ being a positive integer. We shall construct a primitive lth root of unity by means of formula (3.7)(d). For this we construct the objects from the previous section one after the other.

(4.1) *The field K.* For the field K we shall take a field extension $\mathbf{F}_q$ of $\mathbf{F}_{p^h}$ satisfying the conditions stated in (3.4). The first condition, that K contain a primitive lth root of unity, is satisfied by any extension of $\mathbf{F}_{p^h}$, since $p^h\equiv 1 \bmod l$. We just took care of the second condition, that $l-1$ be not divisible by p. The third condition is that for each prime number r dividing $l-1$ the group T_r has an element of order $r^{a(r)}$; by (3.2)(d), this it is equivalent to the requirement that $q^{m_r}\equiv 1 \bmod r^{a(r)}$, where m_r denotes the multiplicative order of q modulo r.

Let m'_r be the multiplicative order of p^h modulo r, and let $b(r)$ be the multiplicative order of $p^{hm'_r}$ modulo $r^{a(r)}$; from $p^{hm'_r}\equiv 1 \bmod r$ it follows that $b(r)$ divides $r^{a(r)-1}$. Now one readily verifies that the number

$$q=p^{h\prod_r b(r)},$$

with r ranging over the primes dividing $l-1$, has the required properties (and in fact, that it is the least power of p^h having these properties). To construct $\mathbf{F}_q$, it suffices to construct an extension of $\mathbf{F}_{p^h}$ of degree $\prod_r b(r)$. By [12, Theorem (9.1)], this can be done within the time bound stated in Theorem 2, provided that for each r with $b(r)>1$ and r not dividing

h an rth degree irreducible polynomial in $\mathbf{F}_{p^h}[X]$ is available; and this is indeed the case, since the given irreducible polynomials g_r in $\mathbf{F}_p[X]$ remain irreducible over $\mathbf{F}_{p^h}$.

(4.2) *The ring A.* We shall work in the ring A constructed in (3.4), with $K = \mathbf{F}_q$, and in the subrings $\mathbf{F}_q[\zeta_r]$ of A. The $\prod_r (r-1)$ elements $\prod_r \zeta_r^{i(r)}$, with $0 \leq i(r) < r-1$, form a basis of A over $\mathbf{F}_q$, the products ranging over the primes dividing $l-1$. Elements of A are represented on this basis. To multiply two basis elements one uses the relations $\sum_{i=0}^{r-1} \zeta_r^i = 0$ (and $\zeta_r^r = 1$). The $\mathbf{F}_q$-dimension of A is at most $l-1$, and the degree of $\mathbf{F}_q$ over $\mathbf{F}_p$ divides $h(l-1)$; so arithmetic in A can be done within the time bound stated in Theorem 2, and the same is true for its subrings $\mathbf{F}_q[\zeta_r]$ and for $\mathbf{F}_q$ itself.

(4.3) *The Teichmüller groups T_r.* For every prime number r dividing $l-1$, one uses [12, Theorem (9.1)] and our hypothesis on the g_r to construct, as above, a field extension of $\mathbf{F}_q$ of degree r; having this field extension, one applies [12, Theorem (5.2)] (with $E = \mathbf{F}_q$) in order to find a generator of T_r. We shall denote it by γ_r; by (3.2), it is a strict root of unity of order equal to the largest power of r that divides $q^{m_r} - 1$.

(4.4) *The group μ.* Raising γ_r to a suitable power one finds an element of T_r of order $r^{a(r)}$, for each r. Taking the product over r one obtains a strict $(l-1)$th root of unity $\zeta \in A^*$. It generates the group that in (3.4) was denoted by μ.

(4.5) *The characters χ.* One next computes an $(l-1) \times (l-1)$ table that for each $\chi \in \Psi$ and each $x \in \mathbf{F}_l^*$ gives the value of $\chi(x)$; so each entry in the table belongs to μ. To do this, one first determines, by trial and error, a primitive root d modulo l; then the characters χ can be numbered by the integers j modulo $l-1$, the value of the jth character at d^i being ζ^{ij}, with ζ as computed in (4.4).

(4.6) *The Jacobi sums $j(\chi, \psi)$.* One computes a second $(l-1) \times (l-1)$ table, giving the Jacobi sums $j(\chi, \psi)$ as elements of A for all χ, $\psi \in \Psi$. This table is computed directly from the definition of Jacobi sums.

(4.7) *Products of Gauss sums.* It is, naturally, not possible to compute the Gauss sums directly from their definition, since η is not available. Instead one proceeds in several steps. In each of these steps one will need to compute certain expressions of the form

$$\prod_{\chi \in \Psi} \tau(\chi, \eta)^{n(\chi)},$$

where the $n(\chi)$ are integers satisfying $\prod_\chi \chi^{n(\chi)} = 1$ (in Ψ). We claim that each such expression can be computed by means of $O\big(\sum_{\chi, n(\chi) \neq 0} \log(|n(\chi)| + 1)\big)$ table look-ups and

multiplications and divisions in A^* and Ψ. To prove this, we first show how to compute an expression of the form $\tau(\chi,\eta)^n/\tau(\chi^n,\eta)$, where n is an integer. If $n=0$ or 1 this equals 1. If n is greater than 1, one sets $m=\lfloor n/2\rfloor$ and uses the formula

$$\frac{\tau(\chi,\eta)^n}{\tau(\chi^n,\eta)} = j(\chi^m,\chi^{n-m})\cdot\frac{\tau(\chi,\eta)^m}{\tau(\chi^m,\eta)}\cdot\frac{\tau(\chi,\eta)^{n-m}}{\tau(\chi^{n-m},\eta)}$$

(which, as all formulas in (4.7), is obtained from (3.7)(b)) to proceed by recursion. To deal with negative n one uses that

$$\frac{\tau(\chi,\eta)^n}{\tau(\chi^n,\eta)}\cdot\frac{\tau(\chi,\eta)^{-n}}{\tau(\chi^{-n},\eta)} = j(\chi^n,\chi^{-n})^{-1}.$$

A general product $\prod_{\chi\in\Psi}\tau(\chi,\eta)^{n(\chi)}$ with $\prod_\chi \chi^{n(\chi)}=1$ is now computed from

$$\prod_{\chi\in\Psi}\tau(\chi,\eta)^{n(\chi)} = \Big(\prod_{\chi\in\Psi}\frac{\tau(\chi,\eta)^{n(\chi)}}{\tau(\chi^{n(\chi)},\eta)}\Big)\cdot\prod_{\chi\in\Psi}\tau(\chi^{n(\chi)},\eta),$$

the value of the last product being obtained from the formula

$$\prod_{i=1}^{t}\tau(\chi_i,\eta) = \prod_{i=2}^{t} j(\chi_1\cdots\chi_{i-1},\chi_i),$$

which is valid whenever $\prod_{i=1}^t\chi_i=1$.

The computation shows that the computed products are independent of the choice of η. This can be seen directly from (3.7)(e).

(4.8) *Gauss sums for characters of prime power order.* Let $\chi\in\Psi$ be a character of order r^t, where r is a prime number and t is a positive integer. We describe how one can compute an element of $\mathbf{F}_q[\zeta_r]$ that is of the form $\tau(\chi,\eta')$, with $\eta'\in\mathbf{F}_q$ a primitive lth root of unity.

First one computes the element $\tau(\chi,\eta)^{r^t}$ of $\mathbf{F}_q[\zeta_r]$ using the method of (4.7), which applies because $\chi^{r^t}=1$. We note that r^t divides $r^{a(r)}$, which in turn divides $q^{m_r}-1$. One now applies the algorithm from (2.6) to the element $\alpha=\tau(\chi,\eta)^{r^t}$ of the ring $R=\mathbf{F}_q[\zeta_r]$, with $m=(q^{m_r}-1)/r^t$ and $n=r^t$, and with γ equal to the generator γ_r of T_r constructed in (4.3). The condition $\alpha^m=1$ from (2.4) is satisfied because of (3.7)(f) and (3.2)(d); and to verify the condition that γ^m be a strict nth root of unity we combine (2.1)(g) with the fact that the order of γ_r is the largest power of r dividing $q^{m_r}-1$. Thus, from the algorithm of (2.6) one obtains an element $\upsilon\in\mathbf{F}_q[\zeta_r]^*$ with $\upsilon^{r^t}=\tau(\chi,\eta)^{r^t}$. Next one

computes the element ϵ defined in (3.8); one can take G to be the least positive integer with $G \equiv g^{r^{t-1}} \bmod r^t$, and the factor $\tau(\chi^G, \eta)/\tau(\chi, \eta)^G$ in the definition of ϵ can be obtained from (4.7). Using ϵ, one computes the element ϑ from (3.8) as well; as was noted in the proof of (3.8), the exponents in the definition of ϑ can be taken modulo r^t. By (3.8), the element $\vartheta \cdot \upsilon$ is now of the desired form $\tau(\chi, \eta')$.

(4.9) *The Gauss sums* $\tau(\chi, \eta)$. For each prime r dividing $l-1$, choose $\chi_r \in \Psi$ of order $r^{a(r)}$, and use (4.8) to compute an element of $\mathbf{F}_q[\zeta_r]$ of the form $\tau(\chi_r, \eta)$; in principle η may depend on r, but Lemma (3.9) shows that there exists a single η that works for all r. Next one puts $\chi_0 = \prod_r \chi_r$, and one computes $\tau(\chi_0, \eta)$ from $\prod_r \tau(\chi_r, \eta)$ by observing that the quotient of these two expressions is computable from (4.7). Starting from $\tau(\chi_0, \eta)$ one computes $\tau(\chi_0^i, \eta)$ for all i (modulo $l-1$) in succession, using that

$$\tau(\chi_0^i, \eta) = \frac{\tau(\chi_0^{i-1}, \eta) \cdot \tau(\chi_0, \eta)}{j(\chi_0^{i-1}, \chi_0)}.$$

Since χ_0 has order $\prod_r r^{a(r)} = l-1$, this gives $\tau(\chi, \eta)$ for all χ and a single η.

(4.10) *The primitive* l*th root of unity* η. To conclude the algorithm, one adds up the $\tau(\chi, \eta)$, for $\chi \in \Psi$, and divides the result by $1-l$. By (3.7)(d), that gives η. It belongs to the subfield $\mathbf{F}_{p^h}$ of $\mathbf{F}_q$, because l divides $p^h - 1$.

This completes our description of the algorithm. The correctness of the algorithm has been proved along the way, and it is straightforward to show that the run time is $(l + h \log p)^{O(1)}$. This proves Theorem 2.

5. Constructing non-residues

In the present section we construct, under suitable conditions, elements of given finite fields that do not belong to certain multiplicative subgroups. In particular, we shall prove Theorem 3. We shall make use of the following result, which is similar to Theorem 3 but much easier to prove.

Theorem (5.1). *There is a deterministic algorithm that, for some positive real number* c*, has the following property: given two prime numbers* p *and* l*, a positive integer* k*, explicit data for* $\mathbf{F}_{p^k}$*, a primitive* l*th root of unity* η *in* $\mathbf{F}_{p^k}$*, and, if* l *does not divide* k*, an irreducible polynomial* g_l *of degree* l *in* $\mathbf{F}_p[X]$*, the algorithm constructs, in time at most* $(l + k \log p)^c$*, an element of* $\mathbf{F}_{p^k}$ *that is not an* l*th power in* $\mathbf{F}_{p^k}$*.*

Proof. We shall write $q = p^k$. As in (4.1), we can use the hypothesis on g_l and [12, Theorem (9.1)] to construct a field extension F of $\mathbf{F}_q$ of degree l. The $\mathbf{F}_q$-linear map $f\colon F \to F$ defined by $f(x) = \sum_{i=0}^{l-1} \eta^{-i} x^{q^i}$ is non-zero, since $f(x)$ may be viewed as a polynomial of degree $(\#F)/q$ in x. Hence, trying the elements of a vector space basis of F over $\mathbf{F}_q$ one by one, one can find an element $\alpha \in F$ with $f(\alpha) \neq 0$. A direct computation shows that $f(\alpha)^q = \eta \cdot f(\alpha)$. This is different from $f(\alpha)$, so we have $f(\alpha) \notin \mathbf{F}_q$ and $F = \mathbf{F}_q(f(\alpha))$. The element $\beta = f(\alpha)^l$ satisfies $\beta^q = \eta^l \beta = \beta$, so $\beta \in \mathbf{F}_q$. Thus, adjoining the lth root $f(\alpha)$ of β to $\mathbf{F}_q$ one obtains the lth degree extension F of $\mathbf{F}_q$. This implies that $X^l - \beta$ is irreducible over $\mathbf{F}_q$, so that β is not an lth power in $\mathbf{F}_q$. This proves (5.1).

The rest of this section is devoted to the proof of Theorem 3. Note the difference between Theorem 3 and Theorem (5.1): in Theorem 3 no polynomial g_l is supposed to be given; instead, one requires a primitive lth root of unity in $\mathbf{F}_{p^k}$ to be given not just for a single l, but for all primes l dividing $\Phi_k(p)$; and the largest of these enters the run time estimate, even when a non-lth-power is constructed only for the smallest.

An important role will be played by elements of order dividing $\Phi_k(p)$ in certain algebras. We begin with a method for constructing such elements, which will also be used in Section 6.

Proposition (5.2). *Let p be a prime number and let k be a positive integer. Let R be an $\mathbf{F}_p$-algebra with the property that the $\mathbf{F}_p$-algebra homomorphism $\sigma\colon R \to R$ that raises every element of R to the power p satisfies $\sigma^k = \mathrm{id}_R$. For each squarefree divisor d of k, write $\sigma_d = \prod_{r|d} \sigma^{k/r}$, the product being computed in the group of automorphisms of R, and r ranging over the primes dividing d. Denote by μ the Möbius function. Then for each $\gamma \in R^*$ the element*

$$\delta = \prod_d \sigma_d(\gamma)^{\mu(d)},$$

the product ranging over the squarefree divisors of k, satisfies $\delta^{\Phi_k(p)} = 1$.

Proof. The definition of δ can be rewritten as

$$\delta = \gamma^{\prod_r (1 - p^{k/r})},$$

the product ranging over the primes dividing k. Since $\Phi_k(p) \prod_r (1 - p^{k/r})$ is divisible by $p^k - 1$ it follows that $\delta^{\Phi_k(p)}$ is a power of $\gamma^{p^k - 1}$, which equals $\sigma^k(\gamma)/\gamma = 1$. This proves (5.2).

Remark. The condition $\sigma^k = \mathrm{id}_R$ in (5.2) is satisfied if R is the product of a collection of fields of cardinality p^k. One can show that, in that case, conversely every $\delta \in R$ with $\delta^{\Phi_k(p)} = 1$ is given by the formula in (5.2), for some $\gamma \in R^*$.

We describe the algorithm that proves Theorem 3. Let p be a prime number, k a positive integer, and write $q = p^k$. We suppose that explicit data for $\mathbf{F}_q$ are given, and that for each prime number l dividing $\Phi_k(p)$ a primitive lth root of unity $\eta_l \in \mathbf{F}_q$ is given. Next we let l be one of these prime numbers. It is our purpose to construct an element of $\mathbf{F}_q$ that is not an lth power in $\mathbf{F}_q$. If l divides k then we can do this by Theorem (5.1). Let it henceforth be assumed that l does not divide k. We claim that in the notation of (5.2) we have

$$\prod_d \sigma_d(\eta_l)^{\mu(d)} \neq 1. \tag{5.3}$$

As we saw in the proof of (5.2), this is the same as saying that the $\prod_r(1-p^{k/r})$th power of η_l is different from 1, i. e., that $\prod_r(1-p^{k/r})$ is not divisible by l. Indeed, from $\Phi_k(p) \equiv 0 \bmod l$ and $k \not\equiv 0 \bmod l$ we see, using (2.2), that $(p \bmod l)$ is a strict kth root of unity in $\mathbf{F}_l$, so that $\prod_r(1 - p^{k/r}) \not\equiv 0 \bmod l$. This proves (5.3).

(5.4) *A reduction.* An element $a \in \mathbf{F}_q^*$ is an lth power in $\mathbf{F}_q$ if and only if $a^{(q-1)/l} = 1$. We claim that it suffices to describe an algorithm that given an element $a \in \mathbf{F}_q^*$ with $a^{(q-1)/l} = 1$ computes an lth root of a in $\mathbf{F}_q$, within time $(s(q) + \log q)^{O(1)}$. Namely, if starting from η_l we take repeatedly lth roots, we will after $O(\log q)$ steps find a root of unity in $\mathbf{F}_q$ whose order is the largest power of l dividing $q - 1$, and this root of unity is not an lth power in $\mathbf{F}_q$. Thus, for the rest of the algorithm, we assume that an element $a \in \mathbf{F}_q$ with $a^{(q-1)/l} = 1$ is given. It is our purpose to find an lth root of a in $\mathbf{F}_q$.

We shall denote by k' the number of squarefree divisors of k; obviously, we have $1 \leq k' \leq k$. If $p < k'l$ then Berlekamp's algorithm for finding a zero of $X^l - a$ is fast enough. Let it now be assumed that $p \geq k'l$.

(5.5) *The ring R.* We shall work in the ring $R = \mathbf{F}_q[X]/(X^l - a)$. Let $\alpha \in R$ denote the residue class of X, so that the elements $1, \alpha, \ldots, \alpha^{l-1}$ form an $\mathbf{F}_q$-basis for R, and $\alpha^l = a$. We have $\alpha^{q-1} = a^{(q-1)/l} = 1$, so the map $R \to R$ that maps each x to x^q is the identity on both $\mathbf{F}_q$ and α, and is therefore the identity; that is, R satisfies the hypothesis of (5.2). Hence all elements of R^* have order dividing $q - 1$.

The ring R has a unique automorphism that is the identity on $\mathbf{F}_q$ and maps α to $\eta_l\alpha$; we denote this automorphism by τ. We have $\tau^l = \mathrm{id}_R$, and τ commutes with the pth power map σ from (5.2) and its powers σ_d. For $\gamma \in R^*$, write $\gamma^{\tau-1} = \tau(\gamma)/\gamma$. For example, we have $\alpha^{\tau-1} = \eta_l$. We claim that:

(5.6) if $\gamma \in R^*$ is such that $\gamma^{\tau-1} \in \mathbf{F}_q^*$, then $\gamma^{\tau-1} \in \langle \eta_l \rangle$.

This follows from $\bigl(\gamma^{\tau-1}\bigr)^l = \prod_{i=0}^{l-1} \gamma^{\tau-1} = \prod_{i=0}^{l-1} \tau^i(\gamma^{\tau-1}) = \tau^l(\gamma)/\gamma = 1$.

(5.7) *A special element of R.* The next step is to construct an element $\beta \in R$ that is either a zero-divisor or satisfies

$$\beta^{\Phi_k(p)} = 1, \qquad \beta^{\tau-1} \notin \mathbf{F}_q^*. \tag{5.8}$$

If $k = 1$ one can take $\beta = 1 + \alpha$, as a simple computation shows. In the general case one finds β by means of a search procedure. First one tests whether there is a zero-divisor among the elements $\alpha + i$, $i = 1, 2, \ldots, k'l - 1$, of R. If so, one is done, so suppose not. Then all these elements are units, and one tries the elements $\prod_d \sigma_d(\alpha + i)^{\mu(d)}$ for the same values of i, the product being as in (5.2). All of these elements have order dividing $\Phi_k(p)$, by (5.2), and we claim that at least one of them satisfies the second condition in (5.8). Suppose not. Then by (5.6) we have

$$\prod_d \Bigl(\frac{\sigma_d(\tau\alpha) + i}{\sigma_d(\alpha) + i}\Bigr)^{l\mu(d)} = 1$$

for all these values of i. Apply the ring homomorphism $R \to \mathbf{F}_q$ that maps α to some lth root b of a; it commutes with the pth power map σ and its powers, so we find that the rational function

$$f = \prod_d \Bigl(\frac{\sigma_d(\eta_l b) + Y}{\sigma_d(b) + Y}\Bigr)^{\mu(d)} \in \mathbf{F}_q(Y)$$

satisfies $f(i)^l = 1$ for $1 \le i < k'l$, and the same is in fact true for $i = 0$. Since f^l is a quotient of two monic polynomials of degree $k'l$, and since all these values of i are pairwise distinct in $\mathbf{F}_p$, it follows that $f^l = 1$ in $\mathbf{F}_q(Y)$, so f is constant. However, we have $f(\infty) = 1$ and $f(0) \ne 1$, by (5.3). This contradiction proves that the search procedure will be successful.

(5.9) *An auxiliary procedure.* We claim that one can construct a zero-divisor in R if an element $\gamma \in R^*$ is known for which the order of $\gamma^{\tau-1}$ is a prime l' dividing $\Phi_k(p)$, but $\gamma^{\tau-1} \notin \langle \eta_l \rangle$; notice that the latter condition is automatic if $l' \ne l$.

To do this, one applies the algorithm of Proposition (2.5) with $\gamma^{\tau-1}$ and $\eta_{l'}$ in the roles of α and ζ, and $n = l'$. This algorithm cannot give rise to an integer i with $\gamma^{\tau-1} = \eta_{l'}^i$, since $\gamma^{\tau-1}$ does by (5.6) not belong to $\mathbf{F}_q$; hence one obtains a non-trivial idempotent e in R, which is the desired zero-divisor.

(5.10) *Constructing a zero-divisor.* If in (5.7) one has not yet been successful in constructing a zero-divisor in R, then one constructs one now. From (5.7) one knows an element $\beta \in R^*$ as in (5.8). We have $\big(\beta^{\tau-1}\big)^{\Phi_k(p)} = 1$, and since the prime factors of $\Phi_k(p)$ are known one can determine the order of $\beta^{\tau-1}$. If it is divisible by some prime $l' \neq l$, then one finds a suitable power γ of β for which $\gamma^{\tau-1}$ has order l', and one applies (5.9) in order to find a zero-divisor. Hence assume that $\beta^{\tau-1}$ has order l^m for some integer $m \geq 0$. By (5.8) we have $m \neq 0$, and if $m = 1$ then by (5.8) one can apply (5.9) to $\gamma = \beta$. Let now $m \geq 2$. In this case, one computes $\xi = (\beta^{\tau-1})^{l^{m-2}}$; this is an element of order l^2, and one has $\xi = \delta^{\tau-1}$ with $\delta = \beta^{l^{m-2}}$. We may assume that $\xi^l \in \langle \eta_l \rangle$, since otherwise one can apply (5.9) to $\gamma = \delta^l$. From $\xi^l \in \langle \eta_l \rangle$ we see that $\epsilon = \xi^{\tau-1}$ satisfies $\epsilon^l = 1$, so again by (5.9) we may assume that $\epsilon \in \langle \eta_l \rangle \subset \mathbf{F}_q$. From $\tau(\delta) = \xi\delta$, $\tau(\xi) = \epsilon\xi$, and $\tau(\epsilon) = \epsilon$ one obtains $\tau^i(\delta) = \epsilon^{\binom{i}{2}}\xi^i\delta$ by induction on i. Since τ has order l it follows that $\delta = \tau^l(\delta) = \epsilon^{\binom{l}{2}}\xi^l\delta$, so $\xi^l = \epsilon^{-\binom{l}{2}}$. By $\xi^l \neq 1$ and $\epsilon \in \langle \eta_l \rangle$ this implies that $l = 2$ and $\epsilon = \eta_2 = -1$. Therefore we have $\xi^2 = -1$ and $\tau(\xi) = -\xi$.

Since all elements of R^* have order dividing $q - 1$, and ξ has order 4, we have $p^k = q \equiv 1 \bmod 4$. We assumed that k is not divisible by l, and $l = 2$, so k is odd and we have $p \equiv p^k \equiv 1 \bmod 4$. Hence one can use Schoof's algorithm [17] to find $\vartheta \in \mathbf{F}_p^*$ with $\vartheta^2 = -1$. Now $(\xi - \vartheta)(\xi + \vartheta) = 0$, and by $\tau(\xi) = -\xi$ neither factor is 0. Thus $\xi - \vartheta$ is a zero-divisor in R.

(5.11) *An lth root of a.* Let $\sum_{i=0}^{l-1} c_i\alpha^i$, with $c_i \in \mathbf{F}_q$, be a zero-divisor in R, as computed in (5.7) or in (5.10). Then one applies Euclid's algorithm to compute $g = \gcd\big(\sum_{i=0}^{l-1} c_i X^i, X^l - a\big)$ in $\mathbf{F}_q[X]$, which is a polynomial of degree n for some n with $0 < n < l$. Each root of g is an lth root of a, so their product, which equals $(-1)^n g(0)$, is an lth root of a^n. Since l is prime, one can find integers u, v with $un + vl = 1$, and then $\big((-1)^n g(0)\big)^u a^v$ is an lth root of a in $\mathbf{F}_q$.

This concludes the description of the algorithm underlying Theorem 3. The correctness has been proved along the way, and it is straightforward to prove the run time bound asserted in the statement of the theorem. This proves Theorem 3.

6. Factoring polynomials

In this section we prove Theorem 1. We begin with three auxiliary results. Let p be a prime number and k a positive integer. We write $q = p^k$.

Lemma (6.1). *The number $\Phi_k(p)$ has a prime divisor l with $l \equiv 1 \bmod k$, unless one is in one of the following cases:*

$$p = 2, \text{ and } k = 1 \text{ or } 6;$$

$$p = 2^m - 1 \text{ for some integer } m \geq 2, \text{ and } k = 2.$$

In all cases one has $s(p^k) \geq k/2$.

Proof. If $k = 1$ then $\Phi_k(p) = p - 1$, and if $k = 2$ then $\Phi_k(p) = p + 1$; in both cases the lemma is easy to check. Next let $k > 2$. If we except the single case $p = 2$, $k = 6$, then by [2, Section 1, Corollary 2] there is a prime number l dividing $p^k - 1$ but not dividing $p^i - 1$ for any positive integer $i < k$. Then l divides $\Phi_k(p)$, and since the multiplicative order of $p \pmod l$ equals k, the order $l - 1$ of the group $\mathbf{F}_l^*$ is divisible by k. The first statement follows, and the second is an immediate consequence. This proves (6.1).

In the proof of the following lemma, and in (6.3), we let σ_d be as defined in Proposition (5.2), with $R = \mathbf{F}_q$; the order of σ_d in the automorphism group G of $\mathbf{F}_q$ equals d. By μ we denote the Möbius function.

Lemma (6.2). *Any vector space basis of $\mathbf{F}_q$ over $\mathbf{F}_p$ contains an element a with $\mathbf{F}_q = \mathbf{F}_p(a)$.*

Proof. Consider the $\mathbf{F}_p$-linear map $g\colon \mathbf{F}_q \to \mathbf{F}_q$ defined by $g(x) = \sum_d \mu(d)\sigma_d(x)$, with d ranging over the squarefree divisors of k. If x belongs to a normal basis of $\mathbf{F}_q$ over $\mathbf{F}_p$, then $g(x) \neq 0$, since the σ_d are pairwise distinct. Hence g is non-zero, and any basis of $\mathbf{F}_q$ over $\mathbf{F}_p$ contains an element a with $g(a) \neq 0$. We can write $g(a) = \big(\prod_r (1 - \sigma_r)\big)a$, with r ranging over the prime divisors of k; the product belongs to the group ring $\mathbf{F}_p[G]$, which naturally acts on the additive group of $\mathbf{F}_q$. Since $1 - \sigma_r$ annihilates the subfield $\mathbf{F}_{p^{k/r}}$ of $\mathbf{F}_q$, and any proper subfield is contained in one of the $\mathbf{F}_{p^{k/r}}$, the product $\prod_r (1 - \sigma_r)$ annihilates all proper subfields. Hence from $g(a) \neq 0$ it follows that a does not belong to any proper subfield of $\mathbf{F}_q$, so that $\mathbf{F}_q = \mathbf{F}_p(a)$. This proves (6.2).

The expression used in the proof of (6.2) is the additive analogue of the expression that appears in (5.2).

One can prove, more precisely, that any basis of $\mathbf{F}_q$ over $\mathbf{F}_p$ contains at least $\varphi(k)$ elements a with $\mathbf{F}_q = \mathbf{F}_p(a)$, where φ denotes the Euler function, and that there is a basis containing exactly $\varphi(k)$ such a's.

Lemma (6.3). *Let $a \in \mathbf{F}_q$ be such that $\mathbf{F}_q = \mathbf{F}_p(a)$, and let t, $u \in \mathbf{F}_p$. Suppose that in the field $\mathbf{F}_q(Y)$ of rational functions one has*

$$\prod_d \big(\sigma_d(a)Y + t\big)^{\mu(d)} = \prod_d \big(\sigma_d(a)Y + u\big)^{\mu(d)},$$

with d ranging over the squarefree divisors of k. Then we have $t = u$.

Proof. If both t and u are 0 we are done. So suppose that $t \neq 0$. We have

$$\Big(\prod_{d,\mu(d)=1} \big(\sigma_d(a)Y + t\big)\Big) \cdot \Big(\prod_{d,\mu(d)=-1} \big(\sigma_d(a)Y + u\big)\Big) =$$
$$\Big(\prod_{d,\mu(d)=1} \big(\sigma_d(a)Y + u\big)\Big) \cdot \Big(\prod_{d,\mu(d)=-1} \big(\sigma_d(a)Y + t\big)\Big).$$

By unique factorization in $\mathbf{F}_q[Y]$, the factor $aY + t$ on the left is proportional to one of the factors on the right. From $\mathbf{F}_q = \mathbf{F}_p(a)$ it follows that the elements $\sigma_d(a)$ are pairwise distinct, so $aY + t$ is not proportional to any of the factors $\sigma_d(a)Y + t$ with $\mu(d) = -1$. Hence there exists d with $\mu(d) = 1$ such that $aY + t$ is proportional to $\sigma_d(a)Y + u$, so that $\sigma_d(a) = (u/t)a$. Applying σ_d we see that $\sigma_d^2(a) = (u/t)\sigma_d(a)$. Also the factor $\sigma_d(a)Y + t$ on the left is proportional to a factor on the right, so the same argument shows that there exists d' with $\mu(d') = 1$ and $\sigma_{d'}(a) = (u/t)\sigma_d(a)$. Then we have $\sigma_{d'} = \sigma_d^2$. Since $\sigma_{d'}$ and σ_d have orders d' and d, respectively, it follows that $d' = d/\gcd(d, 2)$. If d is even then we have $d = 2d'$, which contradicts $\mu(d) = \mu(d') = 1$. Hence d is odd, and we have $d' = d$. From $\sigma_{d'}(a) = (u/t)\sigma_d(a)$ we now see that $u = t$. This proves (6.3).

We turn to the description of the algorithm that proves Theorem 1. Let, for some prime number p and positive integers n and k, a polynomial f over $\mathbf{F}_{p^n}$ be given, as well as an irreducible rth degree polynomial g_r in $\mathbf{F}_p[X]$ for each $r \in R(p^k)$ that does not divide n. It is our purpose to factor f into irreducible factors in $\mathbf{F}_{p^n}[X]$.

The algorithm starts by factoring $\Phi_k(p)$ completely by means of trial division. From $\Phi_k(p) < p^k$ and (6.1) it follows that this can be done in time $\big(s(p^k) + \log p\big)^{O(1)}$.

(6.4) *Preliminary reductions.* Using [5, Section 7.5 and Theorem 7.8.1], one reduces to the case in which f is known to be a product of $\deg f$ pairwise distinct linear factors in $\mathbf{F}_p[X]$,

with $\deg f > 1$. We shall assume that this is the case, so that $X^p \equiv X \bmod f$. Also, we assume that f is monic. Then the coefficients of f and of all of its monic factors belong to $\mathbf{F}_p$.

As in (5.4), we denote by k' the number of squarefree divisors of k. If $p < k'$ or $p = 2$ then Berlekamp's algorithm is fast enough. We shall assume that $p \geq k'$ and that $p \neq 2$.

The algorithm that we describe finds a non-trivial factor of f. Applying the algorithm recursively one obtains the complete factorization of f.

(6.5) *The field* $\mathbf{F}_q$. Let $q = p^k$. If we have $k = 2$ and $p = 2^m - 1$ for some integer $m \geq 2$, then $\mathbf{F}_p[X]/(X^2 + 1)$ is an explicit model for $\mathbf{F}_q$. In the other case one constructs $\mathbf{F}_q$ as follows. Since explicit data for $\mathbf{F}_{p^n}$ are given, one can use [12, Theorem (9.1)] (with $E = \mathbf{F}_p$) to compute an irreducible rth degree polynomial $g_r \in \mathbf{F}_p[X]$ for each prime divisor r of n. Then one knows, with the g_r that were given, an rth degree irreducible polynomial $g_r \in \mathbf{F}_p[X]$ for each $r \in R(p^k)$. From the definition of $R(p^k)$ (see Section 1) and Lemma (6.1) it follows that each prime dividing k belongs to $R(p^k)$. By [12, Theorem (9.1)] one can use the g_r with r dividing k to construct explicit data for $\mathbf{F}_q$.

(6.6) *Special elements of* $\mathbf{F}_q$. One constructs an element $a \in \mathbf{F}_q$ with $\mathbf{F}_q = \mathbf{F}_p(a)$. Such an element may be a byproduct of the construction of $\mathbf{F}_q$ in (6.5) (cf. [12, Theorem (9.1)(b)]); but in any case one can be found among the elements of a basis of $\mathbf{F}_q$ over $\mathbf{F}_p$, by Lemma (6.2). Note that $a \in \mathbf{F}_q$ satisfies $\mathbf{F}_q = \mathbf{F}_p(a)$ if and only if the elements $a, \sigma(a), \ldots, \sigma^{k-1}(a)$ are pairwise distinct, where $\sigma(x) = x^p$.

One also constructs an element $\zeta \in \mathbf{F}_q^*$ of order $\Phi_k(p)$. To do this, one first applies Theorem 2 to $h = k$ in order to find, for each prime number $l \in S(q)$, a primitive lth root of unity in $\mathbf{F}_q^*$. Next, using Theorem 3, one finds for each such l an element γ_l of $\mathbf{F}_q$ that is not an lth power in $\mathbf{F}_q$. A suitable power δ_l of γ_l has order equal to the largest power of l dividing $\Phi_k(p)$. One can now take $\zeta = \prod_l \delta_l$, the product ranging over the primes l dividing $\Phi_k(p)$.

(6.7) *The ring* R. The rest of the algorithm works in the ring $R = \mathbf{F}_q[X]/(f)$. If one knows a zero-divisor in R, then as in (5.11) one can use it in order to find a non-trivial factor g of f in $\mathbf{F}_q[X]$; and as we saw in (6.4), the coefficients of g are in $\mathbf{F}_p$. Thus, it suffices to find a zero-divisor in R.

Let $\sigma\colon R \to R$ denote the pth power map and let $\alpha \in R$ be the residue class of X. We have $\sigma(\alpha) = \alpha$ (see (6.4)), and therefore σ satisfies the condition $\sigma^k = \mathrm{id}_R$ of Proposition (5.2). Let σ_d be as in (5.2). For each d we have $\sigma_d(\alpha) = \alpha$.

If α is a zero-divisor then one is done, so suppose it is not.

(6.8) *A special element of R.* One constructs an element δ of R^* satisfying

$$\delta^{\Phi_k(p)} = 1, \qquad \delta \notin \mathbf{F}_q^*. \tag{6.9}$$

If $k = 1$ then one simply takes $\delta = \alpha$. Let $k > 1$. None of the elements $-ia$ of $\mathbf{F}_q$, with $1 \leq i \leq k' - 1$, belongs to $\mathbf{F}_p$, so none of them is a zero of f; hence for each of these values of i the element $ia + \alpha$ is a unit of R. To find δ, one searches among the elements

$$\prod_d \big(\sigma_d(ia) + \alpha\big)^{\mu(d)}, \qquad 1 \leq i \leq k' - 1.$$

By (5.2), each of these elements is a unit of R of order dividing $\Phi_k(p)$. Hence, to prove that the search is successful, it suffices to prove that at least one of these elements is outside $\mathbf{F}_q^*$. Suppose not; then for each i there exists $c_i \in \mathbf{F}_q^*$ with

$$\prod_d \big(\sigma_d(ia) + \alpha\big)^{\mu(d)} = c_i.$$

Applying, to this equality, two $\mathbf{F}_q$-algebra homomorphisms $R \to \mathbf{F}_q$ that map α to two distinct zeroes t, $u \in \mathbf{F}_p$ of f, we find that

$$\prod_d \big(\sigma_d(a)i + t\big)^{\mu(d)} = \prod_d \big(\sigma_d(a)i + u\big)^{\mu(d)},$$

because both sides are equal to c_i. Thus, the two rational functions occurring in Lemma (6.3) assume the same value at each of $k' - 1$ elements of $\mathbf{F}_q^*$. They also assume the same value at ∞ and at 0, and since each of the two rational functions is the quotient of two polynomials of degrees $k'/2$ they must be the same; but this contradicts (6.3).

We have $k' - 1 = 1$ if k is a prime power, so that in that case no search is necessary.

(6.10) *A zero-divisor.* Finally, one applies (2.5) to $n = \Phi_k(p)$, with δ in the role of α and ζ as constructed in (6.6). The condition $\delta^n = 1$ from (2.3) is satisfied by (6.9), and ζ is a strict nth root of unity in R because it is a primitive nth root of unity in $\mathbf{F}_q$. The algorithm of (2.5) cannot give rise to an integer $i \pmod{\Phi_k(p)}$ with $\delta = \zeta^i$, because $\delta \notin \mathbf{F}_q^*$; hence one obtains a non-trivial idempotent e in R, which is the desired zero-divisor.

This concludes the description of the algorithm underlying Theorem 1. We proved the correctness along the way. The proof of the run time estimate is straightforward; it is useful to note that $k \leq s(q)$ if $p > 2$, by (6.1). This completes the proof of Theorem 1.

References

1. L. M. Adleman, H. W. Lenstra, Jr., *Finding irreducible polynomials over finite fields*, Proc. 18th Annual ACM Sympos. on Theory of Computing (STOC), Berkeley, 1986, pp. 350–355.
2. E. Artin, *The orders of the linear groups*, Comm. Pure Appl. Math. **8** (1955), 355–365.
3. M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969.
4. E. Bach, J. Shallit, *Factoring with cyclotomic polynomials*, Math. Comp. **52** (1989), 201–219.
5. E. Bach, J. Shallit, *Algorithmic number theory*, vol. I, MIT Press, Cambridge, Mass., 1996.
6. E. R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp. **24** (1970), 713–735.
7. S. Evdokimov, *Factorization of polynomials over finite fields in subexponential time under GRH*, pp. 209–219 in: L. M. Adleman, M.-D. Huang (eds), *Algorithmic number theory* (ANTS-I), Lecture Notes in Comput. Sci. **877**, Springer-Verlag, Berlin, 1994.
8. J. von zur Gathen, *Factoring polynomials and primitive elements for special primes*, Theoret. Comput. Sci. **52** (1987), 77–89.
9. M.-D. Huang, *Generalized Riemann hypothesis and factoring polynomials over finite fields*, J. Algorithms **12** (1991), 464–481.
10. S. Lang, *Algebra*, third edition, Addison-Wesley, Reading (Mass.), 1993.
11. H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. **26** (1992), 211–244.
12. H. W. Lenstra, Jr., *Finding isomorphisms between finite fields*, Math. Comp. **56** (1991), 329–347.
13. U. M. Maurer, S. Wolf, *The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms*, SIAM J. Computing **28** (1999), 1689–1721.
14. M. Mignotte, C. Schnorr, *Calcul déterministe des racines d'un polynôme dans un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **306** (1988), 467–472.
15. C. Pomerance, J. Sorenson, *Counting the numbers factorable via cyclotomic methods*, J. Algorithms **19** (1995), 250–265.
16. L. Rónyai, *Factoring polynomials modulo special primes*, Combinatorica **9** (1989), 199–206.

17. R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), 483–494.
18. V. Shoup, *New algorithms for finding irreducible polynomials over finite fields*, Math. Comp. **54** (1990), 435–447.

Computer Sciences Department, University of Wisconsin,
Madison, WI 53706, U. S. A. bach@cs.wisc.edu

Fachbereich Mathematik-Informatik, Universität Paderborn,
33095 Paderborn, Germany gathen@uni-paderborn.de

Department of Mathematics # 3840, University of California,
Berkeley, CA 94720–3840, U. S. A. hwl@math.berkeley.edu
Mathematisch Instituut, Universiteit Leiden,
Postbus 9512, 2300 RA Leiden, The Netherlands hwl@math.leidenuniv.nl