Deterministic Factorization of Polynomials over Special Finite Fields

Eric Bach
Computer Sciences Department
University of Wisconsin
Madison, WI 53706
USA
bach@cs.wisc.edu

Joachim von zur Gathen
Computer Science Department
University of Toronto
Toronto, Ontario M5S 1A4
Canada
gathen@theory.cs.toronto.edu

Hendrik W. Lenstra, Jr.
Department of Mathematics
University of California
Berkeley, California 94720
USA
hwl@math.berkeley.edu

February 28, 1995

Abstract. Let f denote a polynomial of degree n whose coefficients lie in a finite field with q elements and characteristic p. We give a deterministic algorithm to factor such polynomials; assuming the Extended Riemann Hypothesis, its running time is bounded by a polynomial in n, $\log q$, and the largest prime factor of $\Phi_k(p)$, the kth cyclotomic polynomial evaluated at p. In particular, if $p+1$ is smooth, polynomials over fields of characteristic p can be quickly factored without randomization. Thus, there is a deterministic polynomial time algorithm to factor polynomials modulo Mersenne primes.

To be submitted to *Finite Fields and Applications* .

This research was supported by NSF grants DCR-92-08639 [EB], NSERC grant 3-650-126-40, Foundación Andes grant C-10246 [JvzG], and NSF grant DMS-92-24205 [HWL].

1. Introduction.

We present theoretical results on the deterministic complexity of factoring polynomials over large finite fields. This problem can be solved in random polynomial time, but it has no known efficient deterministic algorithm, even if a powerful assumption such as the Extended Riemann Hypothesis (ERH) is made. However, various authors have shown under this hypothesis that fast deterministic algorithms exist to either factor special polynomials or to factor polynomials over special finite fields. Our purpose in this paper is to enlarge the latter category.

Concerning special polynomials, the following is known. Schoof [28] showed that $X^2 - a$ can be factored modulo p deterministically in time polynomial in $|a|$ and $\log p$; if the ERH is true, then the time can be reduced to a polynomial in $\log|a|$ and $\log p$ [2]. (Pila [22] has recently extended this to other polynomials.) This result has been generalized in two directions. Taking a Galois-theoretic approach, Rónyai [27] showed under the ERH that any polynomial in $\mathbb{Z}[X]$ generating a Galois number field can be factored mod p in deterministic polynomial time, except for finitely many exceptional p; this extends results by Huang [16] and Adleman, Manders, & Miller [2], and Evdokimov [13]. Considering the number of factors, Rónyai [25] showed under the same hypothesis that any polynomial modulo p with a bounded number of irreducible factors can be factored deterministically in time bounded by a polynomial in its degree and $\log p$.

Concerning special fields, only the characteristic matters, as Berlekamp [9] showed that factorization of polynomials over a finite field of p^n elements reduces deterministically in polynomial time to factorization over the prime field of integers modulo p. He also showed that the time to factor f modulo p could be bounded by a polynomial in $\deg f$ and p (see [15] for the best current bounds on this time). One of the present authors [14] showed that if the ERH holds and $p-1$ has only small prime factors – in this case we say that $p-1$ is *smooth* – then polynomials can be factored modulo p by a deterministic polynomial time algorithm. This result was obtained independently by Mignotte & Schnorr [21], and extended by Rónyai [26].

In this paper we show that, assuming ERH, polynomials over fields of characteristic p such that $p+1$ is smooth can be factored quickly. More generally, we show this to hold for fields such that for some k, $\Phi_k(p)$, the kth cyclotomic polynomial evaluated at p, is smooth. (The dependence on k is not burdensome). Precise statements of our results can be found in the last theorems of Section 5.

This paper complements the known results on primality testing and integer factorization, to wit: assuming ERH, smoothness of $\Phi_k(p)$, the kth cyclotomic polynomial evaluated at p, leads to fast algorithms to either prove p prime [19] or remove it as a factor from another number n

[6]. By analogy with the Lucas-Lehmer primality test [17], we find that there is an unconditional deterministic polynomial time algorithm to factor polynomials modulo Mersenne primes.

We hasten to point out that our results are purely theoretical, and are directed toward the question of whether there is a deterministic polynomial time algorithm to factor polynomials over finite fields. Settling this question can be viewed as the extreme end of reducing the use of randomness in factorization methods [8]. For this reason we do not attempt to find the most efficient implementations of our methods. For practical purposes the randomized algorithms of Berlekamp [10] and Cantor & Zassenhaus [12] suffice to factor polynomials over any finite field. The asymptotically fastest randomized algorithm is that of von zur Gathen & Shoup [15].

Our algorithm can be summarized as follows. Using standard techniques, we reduce the problem to that of factoring a squarefree polynomial f, whose coefficients and roots are in the field of integers modulo p. Clearly, it will suffice to split f over a larger field K, and we construct K in such a way that its multiplicative group contains a subgroup G of smooth order, simultaneously finding generators for this subgroup. (The order of G will be $\Phi_k(p)$.) Now, by the Chinese remainder theorem, we have

$$K[X]/(f) \cong K \times \cdots \times K,$$

and the group of units of this ring contains a group H isomorphic to $G \times \cdots \times G$. We now find an element x of H that does not lie on the diagonal, and use a process reminiscent of Pohlig & Hellman's index algorithm [23] to find a nontrivial zero-divisor of $K[X]/(f)$. This element leads to a nontrivial factor of f in a straightforward way.

To turn this sketch into a detailed procedure, we must solve two problems. First, we have to efficiently construct K, along with the special elements we need. To make this part of the algorithm run quickly, we need to assume the ERH; however, it can be done once and for all for a given p. Second, we must find elements outside the diagonal. When $k = 2$, we can do this in a direct way, but for general k, we must resort to a search procedure that gives a set of elements, one of which will work.

The rest of this paper is organized as follows. Section 2 collects the algebraic results and notation that we need. Sections 3 and 4 present our constructions for extension fields and off-diagonal elements. The results of these constructions allow us to split f, by generalizing known techniques; we present the details in Section 5. Finally, we discuss the complexity-theoretic import of our results in Section 6, detailing the precise assumptions that our algorithms need.

2. Notation and Background.

The symbol $\mathbb{F}_q$ will denote a finite field containing q elements. If $k > 1$, then by a *model* of $\mathbb{F}_{p^k}$ we shall mean a field of the form $\mathbb{F}_p(\alpha)$, where α is the root of a polynomial of degree k, irreducible over $\mathbb{F}_p$; such a model could be given concretely by specifying the polynomial and p. Any two models of $\mathbb{F}_q$ are isomorphic, as is well-known. We will need the fact that a deterministic polynomial time algorithm exists to find the isomorphism, as was recently shown by one of the present authors [20]. We note that for the purposes of this paper, the algorithm of Evdokimov [13], which assumes the ERH, would also suffice. We could also assume that our finite fields are presented in other ways (for example, by giving generators and an appropriate multiplication table), without affecting our results.

The Galois group of $\mathbb{F}_{q^k}/\mathbb{F}_q$ is cyclic of order k and generated by the *Frobenius automorphism* $\sigma : x \mapsto x^q$. We can easily decide if an element of $\mathbb{F}_{q^k}$ is in $\mathbb{F}_q$ by seeing if $\sigma(x) = x$. If $x \in \mathbb{F}_{q^k}$, then $N(x) = x^{q^{k-1}+\cdots+q+1}$ denotes its *norm*, and $T(x) = x^{q^{k-1}} + \cdots + x^q + x$ its *trace*. Both N and T map $\mathbb{F}_{q^k}$ onto $\mathbb{F}_q$; in addition, T is $\mathbb{F}_q$-linear.

The multiplicative group of any finite field is cyclic, and this fact implies Hilbert's "theorem 90": an element of $\mathbb{F}_{q^k}$ has norm 1 over $\mathbb{F}_q$ if and only if it has the form y/y^σ for some nonzero y in $\mathbb{F}_{q^k}$. The elements of norm 1 form a (cyclic) subgroup of order $q^{k-1} + \cdots + q + 1$ in the multiplicative group of $\mathbb{F}_q$.

$\mathbb{F}_q[X]$ denotes the polynomial ring in one indeterminate over $\mathbb{F}_q$; if σ is an automorphism of $\mathbb{F}_q$, we let σ act on $\mathbb{F}_q[X]$ by transforming coefficients but leaving X untouched. Using this device, the definitions of norm and trace extend to polynomials as well. If the coefficients of f belong to the fixed field of σ, then this automorphism acts on $\mathbb{F}_q[X]/(f)$.

Φ_r will denote the rth cyclotomic polynomial; if r is prime then

$$\Phi_r(X) = X^{r-1} + \cdots + X + 1.$$

We shall let C_m denote a cyclic group of order m. If $m = m_1 \cdots m_r$ is a relatively prime factorization, then

$$C_m \cong \prod_{i=1}^{r} C_{m_i},$$

with the projection onto the ith component given by $x \mapsto x^{m/m_i}$.

By the ERH we mean the following statement: the Dedekind zeta-function of a number field K has no zeroes in the half plane $\mathrm{Re}(s) > 1/2$. (See [13] and [16] for more details on implications of the ERH.)

For positive integers n, we let $S_k(n)$ denote the largest prime factor of $\Phi_k(n)$; thus $S_1(p)$ is the largest prime divisor of $p-1$, $S_2(p)$ the largest prime divisor of $p+1$, and so on. As usual $p^e || m$ means that p^e, but not p^{e+1}, divides m.

3. Constructing extension fields.

This section gives an algorithm to find a model of $\mathbb{F}_{p^k}$, together with an element outside the subgroup of rth powers for each prime r dividing $\Phi_k(p)$. While techniques to do this are readily available in the literature, the precise result we shall need seems not to be. Assuming ERH, the algorithm's running time is bounded by a polynomial in $\log p$ and the largest prime factor of $\Phi_k(p)$.

Algorithm 3.1.

Input: p^k, an odd prime power; r, a prime divisor of $p^k - 1$.

Output: K, a model of $\mathbb{F}_{p^k}$; η, an element of $K - K^r$.

Let $m = kr$.
Let $L = \mathbb{F}_p(\alpha)$ be a model of $\mathbb{F}_{p^m}$.
Let T denote the trace from L to $\mathbb{F}_{p^k}$.
Choose i, $0 \le i < m$, so that $\tau = T(\alpha^i)$ generates $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$.
Let $K = \mathbb{F}_p(\tau)$.
Let $\zeta \in K$ be a root of Φ_r;
Let $\beta = \alpha + \zeta\alpha^{p^k} + \ldots + \zeta^{r-1}\alpha^{p^{k(r-1)}}$.
Return K and $\eta = \beta^r$.

Theorem 3.2 [ERH]. Algorithm 3.1 correctly constructs K and η. It uses $(k + r + \log p)^{O(1)}$ steps.

Proof. We first show correctness. We first claim that some α^i has a trace generating $\mathbb{F}_{p^k}/\mathbb{F}_p$. To see this, consider the $\mathbb{F}_p$-vector space generated by the proper subfields of $\mathbb{F}_{p^k}$. By inclusion-exclusion, the dimension of this space is

$$\sum_{\substack{d|k \\ d \neq k}} \mu(k/d)d = k - \varphi(k) < k.$$

The trace is an $\mathbb{F}_p$-linear mapping from L onto $\mathbb{F}_{p^k}$, so for some i, $T(\alpha^i)$ will lie outside this subspace and hence outside every proper subfield of $\mathbb{F}_{p^k}$. This proves the claim. Since $r \mid p^k - 1$, $\mathbb{F}_{p^k}$ contains a primitive rth root of unity ζ. Now α generates $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^k}$, and this is a cyclic extension whose degree r is relatively prime to p. β is the Lagrange resolvent, and by a classical theorem of algebra [33, §55], β^r is in $\mathbb{F}_{p^k}$ and β generates $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^k}$. It follows that η is in $\mathbb{F}_{p^k}$, but not an rth power.

As for the running time, we must check that all the field-theoretic constructions can be done in polynomial time. The construction of L can be done with the algorithm of Adleman & Lenstra [1], which assuming ERH finds an irreducible polynomial of degree m over $\mathbb{F}_p$ in $O(m + \log p)^{O(1)}$ steps. The construction of K uses linear algebra to find the minimal polynomial for τ. Finally, we can factor Φ_r over $\mathbb{F}_{p^k}$ and find ζ in polynomial time under the ERH with known algorithms [16, 25]. ■

We remark that as an alternative to explicitly constructing a Lagrange resolvent, one can solve linear equations over $\mathbb{F}_p$. In fact, any $x \in K^*$ satisfying $x^{p^k} = \zeta x$ can be used in place of β.

We now need a lemma on cyclotomic polynomials, which shows that we can afford to spend time polynomial in k.

Lemma 3.3. If p is an odd prime, then $k \leq S_k(p)$.

Proof: Clearly this holds for $k \leq 2$, so we may as well assume that $k > 2$. Then there is a prime q dividing $p^k - 1$, but no $p^i - 1$ for $i < k$ (see, e.g. [4], Corollary 2). Such a q divides $\Phi_k(p)$, and since q is prime, it follows from Fermat's theorem that q does not divide k. Then we must have $q \equiv 1$ modulo k, from which the result follows. ■

Theorem 3.4 [ERH]. A model of $\mathbb{F}_{p^k}$, together with a non-rth-power for every prime r dividing $\Phi_k(p)$, can be constructed in $(S_k(p) + \log p)^{O(1)}$ steps.

Proof. If $k = 1$, we may use Ankeny's theorem [3], which states that $\mathbb{F}_p^*$ is generated by the first $O(\log p)^2$ positive integers. (It is proved in [5] that the primes $\leq 2(\log p)^2$ suffice.) Otherwise, factor $\Phi_k(p)$, then run algorithm 3.1 using each prime r dividing $\Phi_k(p)$. Combine the models using the algorithm of [20]. ■

4. Constructing off-diagonal elements.

In this section, f will denote a squarefree polynomial in $\mathbb{F}_p[X]$, of degree greater than 1, all of whose roots lie in $\mathbb{F}_p$. We let $K = \mathbb{F}_p(\alpha)$ denote a model of $\mathbb{F}_{p^k}$. The multiplicative group K^* contains a unique subgroup G of order $\Phi_k(p)$; we let H denote the subgroup of $R^* = K[X]/(f)^*$ of elements all of whose components lie in G. That is, $H = G \times \cdots \times G$, so that $H = \{x \in R : x^{\Phi_k(p)} = 1\}$. It will be convenient to introduce the set $I = H - K$. These elements will be useful in factoring f.

In this section, we give deterministic polynomial-time constructions for elements in I. Because our goal is to factor f, we may as well assume that p is odd, and that $k < p$, because otherwise known deterministic factoring algorithms can be used.

If $k = 1$, we have $I = R^* - K$; any nonconstant polynomial can be used. If $k = 2$, a construction can be based on the following lemma.

Lemma 4.1. Let $K = \mathbb{F}_p(\alpha)$ be a model of $\mathbb{F}_{p^2}$, and let $\sigma : K \to K$ denote the Frobenius automorphism. In $R = K[X]/(f)$, the element $a = (X+\alpha)/(X+\alpha^\sigma) \bmod f$ is a unit of order dividing $p+1$, and does not belong to K. That is, $a \in I$.

Proof: Because f has all of its roots in $\mathbb{F}_p$, $X+\alpha$ and $X+\alpha^\sigma$ will be nonzero modulo each irreducible factor of f. Therefore $a \in R^*$. We note that the exponent of R^* is p^2-1, since R is the direct sum of copies of K. Since a is a $1-p$th power, we have $a^{p+1} = 1$. To show that a does not belong to K, it will suffice to show that $\phi : \mathbb{F}_p \to K$ defined by $\phi(x) = (x+\alpha)/(x+\alpha^\sigma)$ is injective. To do this, choose x and y in $\mathbb{F}_p$, and assume that $(x+\alpha)/(x+\alpha^\sigma) = (y+\alpha)/(y+\alpha^\sigma)$. Clear fractions, subtract common terms, and rearrange to find that $x(\alpha-\alpha^\sigma) = y(\alpha-\alpha^\sigma)$. Since α generates K, $\alpha \neq \alpha^\sigma$, so $x = y$. ∎

More generally, this construction works when k is prime, and it can be easily extended to cover the case where k is a prime power. However, to get a method that works for all k, we must give up the idea that a particular element can be chosen *a priori* from I. Rather, we resort to a "search procedure" that constructs a small number of elements, one of which belongs to I. The search procedure is based on the following idea. In general, we get elements whose $\Phi_k(p)$th powers are 1 by raising elements of H to the $(p^k-1)/\Phi_k(p)$ power. If k is prime, it is easy to get elements of I this way, because $(p^k-1)/\Phi_k(p) = p-1$. In general, however, we do not have such good control over $\Phi_k(p)$'s cofactor, and the job becomes much easier if we replace it by its multiple $\prod_r(1-p^{k/r})$, where r runs over the prime divisors of k. Intuitively, it is clear that raising to this power will have the same effect, because this removes everything from K^* except elements whose order divides $\Phi_k(p)$. Furthermore, an element raised to this new power is a rational function of its conjugates; this simple form allows us to prove that the search will be successful.

We formalize these remarks with the following result; it contains Lemma 4.1 as a special case.

Lemma 4.2. Let $1 < k < p$, and let k' denote the number of squarefree divisors of k. Let $\Psi(p) = \prod_r(1-p^{k/r})$, where r is restricted to prime divisors of k. Let $K = \mathbb{F}_{p^k} = \mathbb{F}_p(\alpha)$ and assume $f \in \mathbb{F}_p[X]$ is squarefree, of degree ≥ 2, and has all roots in $\mathbb{F}_p$. Then in $R = K[X]/(f)$, we have $(X+i\alpha)^{\Psi(p)} \in K$ for at most $k'-2$ elements $i \in \mathbb{F}_p^*$.

Proof. We assume that $k'-1$ elements of $\mathbb{F}_p^*$ have the property, and derive a contradiction.

Choose two distinct zeroes t, u of f in $\mathbb{F}_p$. If $(X+i\alpha)^{\Psi(p)} \in K$, we have

$$(X+i\alpha)^{\Psi(p)} \bmod X-t = (X+i\alpha)^{\Psi(p)} \bmod X-u,$$

so

$$(t+i\alpha)^{\prod_r(1-p^{k/r})} = (u+i\alpha)^{\prod_r(1-p^{k/r})}.$$

We will rewrite this in terms of the Frobenius automorphism σ, which sends each element in K to its pth power. Let $\sigma_d = \prod_{r|d} \sigma^{k/r}$, where r ranges over prime divisors of d; if d is squarefree then σ_d is an automorphism of order d. After expanding $\prod_r(1-p^{k/r})$ in powers of p, the above equality becomes

$$\prod_{d|k}(i\alpha^{\sigma_d}+t)^{\mu(d)} = \prod_{d|k}(i\alpha^{\sigma_d}+u)^{\mu(d)}.$$

where μ denotes the Möbius function. Therefore, if $(X+i\alpha)^{\Psi(p)} \in K$, for $k'-1$ values of i, the polynomial $g \in \mathbb{F}_{q^k}[Y]$, given by

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

has $k'-1$ zeroes. We also have $g(0)=0$, because the constant terms cancel, so g has at least k' zeroes. But the degree of g is less than k', since the leading terms cancel; this and the bound $k' \le k < p$ shows that g is identically zero:

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

We may assume that $t \neq 0$. The factor $Y\alpha+t$ on the left must be proportional to one of the factors on the right. From $K=\mathbb{F}_p(\alpha)$ it follows that the elements $\sigma_d(\alpha)$ are pairwise distinct, so $Y\alpha+t$ is not proportional to any of the factors $Y\sigma_d(\alpha)+t$ with $\mu(d)=-1$. Hence there exists d with $\mu(d)=1$ such that $Y\alpha+t$ is proportional to $Y\sigma_d(\alpha)+u$, so that $\sigma_d(\alpha)=(u/t)\alpha$. Applying σ_d we see that $\sigma_d^2(\alpha)=(u/t)\sigma_d(\alpha)$. Also the factor $Y\sigma_d(\alpha)+t$ on the left must be proportional to a factor on the right, so the same argument shows that there exists d' with $\mu(d')=1$ and $\sigma_{d'}(\alpha)=(u/t)\sigma_d(\alpha)$. Then we have $\sigma_{d'}(\alpha)=\sigma_d^2(\alpha)$, so $\sigma_{d'}=\sigma_d^2$. We now observe that the orders of σ_d and σ_d' are $\mathrm{lcm}_{r|d}\{k/r\}$ and $\mathrm{lcm}_{r|d'}\{k/r\}$, respectively. So, if $\sigma_{d'}=\sigma_d^2$, it must be the case that $d'=d/\gcd(d,2)$. If d is even then $d=2d'$, which contradicts $\mu(d)=\mu(d')=1$. If d is odd then $d'=d$, so from $\sigma_{d'}(\alpha)=(u/t)\sigma_d(\alpha)$ we obtain the contradiction $u=t$. ■

Theorem 4.3. Under the assumptions of Lemma 4.2, at least one of the elements $(X + i\alpha)^{(p^k-1)/\Phi_k(p)}$, $i = 1, \ldots, k'-1$ belongs to I.

Proof. We note that

$$\Psi_k(p) = (p^k - 1)/\Phi_k(p) \mid \prod_r (p^{k/r} - 1),$$

when r ranges over the prime divisors of k. Certainly all $k'-1$ elements are units, and if they all belonged to K, we would have $(X + i\alpha)^{\prod_r (1-p^{k/r})} \in K$, for $i = 1, \ldots, k'$, contradicting Lemma 4.2. ■

5. Factoring with off-diagonal elements.

In this section we give a deterministic algorithm to factor polynomials over $\mathbb{F}_p$.

It is known that the problem of polynomial factoring over any finite field of characteristic p can be reduced deterministically in polynomial time to factoring over the prime field, and even to finding roots of squarefree polynomials that split completely over the prime field [9, 10]. The reduction can be arranged so that the degree of the new polynomial does not exceed that of the old. (See, e.g. [7, p. 143].) Factoring polynomials of this special type is the problem we will actually solve.

Hence consider a polynomial $f \in \mathbb{F}_p[X]$ of degree l, with l distinct roots in $\mathbb{F}_p$. Let $k \geq 1$. We assume available a model of $\mathbb{F}_{p^k}$ as $\mathbb{F}_p(\alpha)$, as well as a non-rth-power in $\mathbb{F}_{p^k}$ for each prime r dividing $\Phi_k(p)$. Our algorithm actually splits f in $\mathbb{F}_{p^k}[X]$; since f has all its roots in $\mathbb{F}_p$, any factor thus found must lie in $\mathbb{F}_p[X]$.

Algorithm 5.1.

Input: f, a polynomial in $\mathbb{F}_p[X]$ with distinct linear factors; $\mathbb{F}_p(\alpha)$, a model of $\mathbb{F}_{p^k}$, and for each prime r dividing $\Phi_k(p)$, an element $\eta \in \mathbb{F}_p(\alpha) - \mathbb{F}_p(\alpha)^r$.

Output: A nontrivial factor of f.

Obtain an element $d(X) \in I$ (using Lemma 4.1 or Theorem 4.3).

For each prime r dividing $\Phi_k(p)$:

  Find s so that $r^s \,||\, \Phi_k(p)$.

  Choose $\eta \in \mathbb{F}_{p^k} - \mathbb{F}_{p^k}^r$, and let $\gamma = \eta^{(p^k-1)/r^s}$, $\zeta = \gamma^{r^{s-1}}$.

  Set $v(X) = d(X)^{\Phi_k(p)/r^s} \bmod f(X)$.

  For $i = 0, \ldots, s-1$:

    Let $w(X) = v(X)^{r^{s-(i+1)}} \bmod f(X)$.

    If $w(X) \in \mathbb{F}_{p^k}$ (a constant) then:

      Find $e_i < r$ such that $\zeta^{e_i} \equiv w(X) \bmod f(X)$.

      Replace $v(X)$ by $v(X)/\gamma^{e_i r^i}$.

    Otherwise, find j, $0 \le j < r$, such that $\gcd(v(X) - \zeta^j, f(X))$ splits $f(X)$.

Theorem 5.2. If $f \in \mathbb{F}_p[X]$ has distinct linear factors, and $\deg f > 1$, then Algorithm 5.1 finds a nontrivial factor of f. Its running time is $(\deg f + \log p + S_k(p))^{O(1)}$.

Proof. G, the group of order $\Phi_k(p)$ in $\mathbb{F}_{p^k}$, is isomorphic to $\prod_r C_{r^s}$, with the projection onto the rth factor given by $x \to x^{\Psi_k(p)/r^s}$. (Recall that C_m denotes a cyclic group of order m.) Since η is not an rth power, γ generates C_{r^s} and ζ is a primitive rth root of unity.

Let $f_1(X), \ldots, f_l(X)$ be the linear factors of $f(X)$; for $i = 1, \ldots, l$, let d_i denote $d(X)$ modulo $f_i(X)$. By the definition of I, we know that no d_i is zero, and each d_i belongs to G. Consider the first r (one has to exist) for which the projections of the d_i into C_{r^s} differ; we can choose indices so that

$$v_1 = d_1^{\Psi_k(p)/r^s} \ne d_2^{\Psi_k(p)/r^s} = v_2.$$

Since γ is a generator, any element of C_{r^s} has a representation

$$\gamma^{e_0 + e_1 r + \cdots + e_{s-1} r^{s-1}}$$

with $0 \le e_i < r$. Find the least i such that the ith such "digits" of v_1 and v_2 disagree. Then when the inner loop is entered at step i, we will have

$$v_1 = v(X) \bmod f_1(X) = \gamma^{e_i^{(1)} r^i + \cdots}$$

$$v_2 = v(X) \bmod f_2(X) = \gamma^{e_i^{(2)} r^i + \cdots}$$

with $e_i^{(1)} \ne e_i^{(2)}$. Then

$$w_1 = w(X) \bmod f_1(X) = \gamma^{e_i^{(1)} r^{s-1}} = \zeta^{e_i^{(1)}}$$

and

$$w_2 = w(X) \bmod f_2(X) = \gamma^{e_i^{(2)} r^{s-1}} = \zeta^{e_i^{(2)}}$$

so the last line of the algorithm will split f. ■

Theorem 5.3 [ERH]. Let $\mathbb{F}_q$ be a field of characteristic p, and let $S_k(p)$ denote the largest prime factor of $\Phi_k(p)$. There is an algorithm with the following property: when presented with a polynomial $f \in \mathbb{F}_q[X]$ of degree n, it factors f in $O(n + S_k(p) + \log q)^{O(1)}$ steps.

Proof. Combine theorem 5.2, the results of the last section, and the remarks on factoring polynomials over extension fields. ■

When $k = 2$, our results have the following curious application.

Corollary 5.4. There is a deterministic polynomial time algorithm that factors polynomials over $\mathbb{F}_p$, when p is a Mersenne prime (i.e., equal to $2^s - 1$ for an odd prime s).

Proof. As $p + 1 = 2^s$, the only thing to check is that we can deterministically construct a model of $\mathbb{F}_{p^2}$ together with a nonsquare. Hence let $f(X) = X^2 - 2^{(p+1)/2}X - 1$. The discriminant of f is a quadratic nonresidue mod p, and if η is a root of it, then $\eta^{2^s} = -1$, so η is not a square (see [18]). Hence the required model is $\mathbb{F}_p(\eta)$. ■

No one has shown that there are infinitely many Mersenne primes, but this seems likely from density considerations (see [30], p. 197). Because there is a deterministic polynomial-time test for Mersenne primes, we can therefore conjecture that the set of p for which factorization modulo p is "easy" contains an infinite polynomial-time recognizable subset.

Solved by Shparlinskii?.

6. Using primitive roots to construct nonresidues.

We have used the ERH in two ways: to construct an extension field $K = \mathbb{F}_{p^k}$, and to construct generators for K^*. Thus, the ERH could be replaced by (unproved) assumptions that the above two problems can be solved in deterministic polynomial time. For the case $k = 1$, Rónyai [26] has shown that it is sufficient to have generators for the *socle* of $\mathbb{F}_p^*$, that is, a primitive r-th root of unity for every prime divisor of $p - 1$. In this section we generalize this theorem to arbitrary k. It is simplest to treat $k = 1$ first.

Theorem 6.1. [Rónyai] There is a deterministic algorithm that, when given primitive r-th roots of unity in $\mathbb{F}_p$ for every prime $r \mid p - 1$, finds rth power nonresidues for each such r in $(S_1(p) + \log p)^{O(1)}$ steps.

Proof. We can construct an r-th power nonresidue by repeatedly taking r-th roots. We can get an r-th root of $e \in (\mathbb{F}_p^*)^r$ from a nontrivial monic factor g of the polynomial $f = X^r - e$, as follows. Suppose g has degree $n < r$. Since $X^r - e$ splits in $\mathbb{F}_p$, g is a product of linear polynomials $X - a$, with $a^r = e$. Then $\delta = (-1)^n g(0)$ is an rth root of e^n, and if $sr + tn = 1$, $\delta^t e^s$ is an rth root of e.

Our goal is therefore to find a zero-divisor $d(X)$ in the ring $R = \mathbb{F}_p[X]/(f)$, because in this case $\gcd(d(X), f(X))$ is a nontrivial factor of f.)

Let τ denote the automorphism of R defined by $X^\tau = \zeta X$, where $\zeta \in \mathbb{F}_p$ is a primitive rth root of unity. We identify R with $\mathbb{F}_p \times \mathbb{F}_p \times \cdots \times \mathbb{F}_p$, in such a way that τ permutes components cyclically. ¿From this we can see that a "coboundary" $\gamma^{\tau-1} = \gamma^\tau/\gamma$ lies in $\mathbb{F}_p^*$ iff it is a power of ζ.

Let $\beta = 1 + X$. If this is not a unit we already have a factor of f, so assume it is. Within our time bound we can factor $p - 1$ and find the order of $\beta^{\tau-1}$. If the order is not a power of r, some power of $\beta^{\tau-1}$ will have prime order $r' \neq r$; since this is also a coboundary it cannot be in $\mathbb{F}_p$, and we can use it to split f as in Algorithm 5.1. If the order is r, a direct calculation shows that $\beta^{\tau-1} = (1 + \zeta X)/(1 + X) \notin \mathbb{F}_p$, so we can also use it to split f.

The only remaining possibility is that $\beta^{\tau-1}$ has order r^m with $m \geq 2$. If this is the case, choose a power $\xi = \gamma^{\tau-1}$ with order r^2. We can assume that both ξ^r and $\epsilon = \xi^{\tau-1}$ lie in $\mathbb{F}_p^*$ (since both have order r, we get a zero-divisor otherwise). Because $\gamma^\tau = \xi\gamma$, $\xi^\tau = \epsilon\xi$, and $\epsilon \in \mathbb{F}_p$, we must have $\gamma = \gamma^{\tau^r} = \epsilon^{\binom{r}{2}}\xi^r\gamma$. Because $\epsilon^r = 1$ and $\xi^r \neq 1$, this is impossible unless $r = 2$.

So we can assume $r = 2$. If $\beta^{\tau-1}$ has order 4, we get a zero divisor from this element or its square. (Its square has order 2 and will lead to a zero-divisor unless it equals -1. In the latter case, we find that $(1 + X^2) = -(1 + X^2)$, so for odd p $(1 + X^2)$ is a nonunit.) If not, its order must be a multiple of 8. As before, choose a power ξ to have order exactly 8. If $\xi^4 \neq -1$, this is outside $\mathbb{F}_p$ and we get a zero divisor. Otherwise, we observe that $\xi^2 \notin \mathbb{F}_p$ (since all coboundaries in $\mathbb{F}_p$ have order dividing 2). Let $\theta = \sqrt{-1}$ in $\mathbb{F}_p$ (this can be obtained via Schoof's algorithm [28]); then $\xi^2 - \theta$ is a zero divisor. ■

We now extend the above argument to cover $k > 1$.

Theorem 6.2. Let K be a model of $\mathbb{F}_q$, with $q = p^k$, and assume we are given primitive r-th roots of unity in $\mathbb{F}_q$ for every prime $r \mid \Phi_k(p)$. There is a deterministic algorithm to find rth power nonresidues, for each such r, using $(S_k(p) + \log p)^{O(1)}$ steps.

Proof. It is convenient to deal first with the case that $r \mid k$. If r is odd, we can use Lagrange resolvents (as in Algorithm 3.1) to get an r-th power nonresidue in K. If $r = 2$, the Lagrange resolvent will still not be a r-th power, unless $k = 2k'$ with k' odd, and $p \equiv 3 \bmod 4$. [**Reference?**] But in this case, $(\frac{-1}{p}) = -1$, and we can use Tonelli's algorithm [31] to deterministically solve quadratic equations in $\mathbb{F}_p$, hence (using a reduction that does not increase degree) in $\mathbb{F}_q$.

We now observe that that if $r = 2$ and k is odd, then r cannot divide $\Phi_k(p)$, when $p > 2$. For, if it did, there would be some prime ρ dividing k for which $r \mid (1 - p^{k/\rho})$, that is, $p^{k/\rho} \equiv 1 \bmod r$. We would then have

$$\frac{1-p^k}{1-p^\rho} = \sum_{i=0}^{r-1} p^{ik/\rho} \equiv \rho \not\equiv 0$$

mod r, contradicting $r \mid \Phi_k(p)$.

Hence we have only to construct r-th power nonresidues in K, for odd r. As above, this reduces to finding zero divisors in rings of the form $R = K[X]/(X^r - e)$. We can do this as in the proof of Theorem 6.1 (for $k = 1$) provided that we know an element $\beta \in R$ satisfying the following two conditions: (i) β is a unit of R, whose order divides $\Phi_k(p)$, and (ii) $\beta^{\tau-1}$ is not a power of ζ in R. (As above, we let $X^\tau = \zeta X$, where ζ is a primitive rth root of unity in K.)

We will not construct β directly but only provide a search procedure. (This is similar to the proof of Theorem 4.3.) Let k have k' squarefree divisors. We may assume that $p > k'r$. We now show there is some i, $1 \le i \le k'r$, such that

$$\beta_i = (X+i)^{\prod_\rho (1-p^{k/\rho})}$$

satisfies (i) and (ii), or lies outside R^*.

Property (i) holds for all i, because $\Phi_k(X)\prod_{\rho|k}(X^{k/\rho} - 1)$ is a multiple of $X^k - 1$.

To prove (ii), it is easy to prove a stronger condition, namely that $(\beta_i^{\tau-1})^r \ne 1$ in R. If this cannot be done, then

$$(\zeta X + i)^{r\prod_\rho (1-p^{k/\rho})} = (X+i)^{r\prod_\rho (1-p^{k/\rho})}$$

holds in R. Therefore it also holds if we replace X by a, an rth root of e in K. We see then that the rational function

$$f(Z) = \prod_d \left(\frac{(\zeta a)^{\sigma_d} + Z}{a^{\sigma_d} + Z}\right)^{\mu(d)r},$$

where d ranges over squarefree divisors of k, equals 1 whenever its argument is an integer in the range $1, \ldots, k'r$. (We define μ and σ_d as in the proof of Theorem 4.3.) By considering degrees we see that f must be identically 1. This implies, then, that its rth root

$$\prod_d \left(\frac{(\zeta a)^{\sigma_d} + Z}{a^{\sigma_d} + Z}\right)^{\mu(d)}$$

must also be 1 (consider the leading coefficients in Z). From the constant coefficient we get that

$$\prod_d (\zeta^{\sigma_d})^{\mu(d)} = 1,$$

so that r divides $\prod_\rho(1 - p^{k/\rho})$. This is a contradiction. ■

7. Comments.

In this section we collect some miscellaneous comments on our results.

1. Although our discussion above used the base field $\mathbb{F}_p$, everything could have been done relative to $\mathbb{F}_q$, where $q = p^e$. This might be preferable in certain cases. For example, if $p = 157$ and $q = p^2$, then $29 = S_2(q) < 79 = S_2(p)$. We note that such cases are rare, and will not happen when $\Phi_k(X) \mid \Phi_k(X^e)$.
2. The last line of Algorithm 5.1 involves a search through $r \le S_k(p)$ polynomials. Therefore we can give its running time (in bit operations) as $S_k(p)(\deg f + \log p)$. As remarked by Buchmann & Shoup [11], one could use the Fast Fourier transform to reduce the dependence on $S_k(p)$ to $\sqrt{S_k(p)}$. The technique is similar to that of the Pollard-Strassen factoring algorithm.
3. The density of primes p for which $S_k(p)$ is smooth is not known. Data collected by Pomerance & Sorenson [24] suggests that for large p, $p \pm 1$ is smooth with roughly the same chance as a random number of the same size.

Acknowledgements. We wish to thank the Information Technology Research Centre, Province of Ontario, for sponsoring a visit by the first author to the University of Toronto. We would also like to thank the United States National Science Foundation and the National Science and Engineering Research Council of Canada for their support.

References.

1. L.M. Adleman and H.W. Lenstra, Jr., Finding irreducible polynomials over finite fields, Proceedings of the 18th ACM Annual ACM Symposium on Theory of Computing (1986).
2. L. Adleman, K. Manders, and G. Miller, On taking roots in finite fields, Proceedings of the 18th Annual IEEE Symposium on Foundations of Computer Science (1977), pp. 175-178.
3. N. C. Ankeny, The least quadratic non residue, Annals of Mathematics 55, pp. 65-72, 1952.
4. E. Artin, The orders of the linear groups, Communications on Pure and Applied Mathematics 8 (1955), pp. 355-365.
5. E. Bach, Explicit bounds for primality testing and related problems, Mathematics of Computation 55, pp. 355-380 (1990).
6. E. Bach and J. Shallit, Factoring with cyclotomic polynomials, Mathematics of Computation 52, pp. 201-219 (1989).

7. E. Bach, Number-theoretic algorithms, Annual Review of Computer Science 4, pp. 119-172 (1990).
8. E. Bach and V. Shoup, Factoring polynomials with fewer random bits, J. Symbolic Computation 9, pp. 229-239 (1990).
9. E.R. Berlekamp, Factoring polynomials over finite fields, Bell System Technical Journal 46 (1967), pp. 1853-1859.
10. E.R. Berlekamp, Factoring polynomials over large finite fields, Mathematics of Computation 24 (1970), pp. 713-735.
11. J. Buchmann and V. Shoup, Constructing nonresidues in finite fields and the extended Riemann hypothesis, Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, pp. 72-79 (1991).
12. D. Cantor and H. Zassenhaus, Factoring polynomials over finite fields, Mathematics of Computation 36, pp. 587-592 (1981).
13. S.A. Evdokimov, Factorization of a solvable polynomial over finite fields and the generalized Riemann hypothesis, Zapiski Nauchnyck Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta imeni V.A. Steklova Akademii Nauk SSSR (LOMI) 176 (1989), Teor. Slozhn. Vychisl. 4, 104-117, 153.
14. J. von zur Gathen, Factoring polynomials and primitive elements for special primes, Theoretical Computer Science 52, pp. 77-89 (1987).
15. J. von zur Gathen and V. Shoup, Computing Frobenius maps and factoring polynomials, Computational Complexity 2, pp. 187-224 (1992).
16. M.-D. Huang, Riemann hypothesis and finding roots over finite fields, Proceedings of the 17th Annual ACM Symposium on Theory of Computing, pp. 121-130 (1985).
17. D. H. Lehmer, An extended theory of Lucas' functions, Annals of Mathematics 31, pp. 419-448 (1930).
18. H.W. Lenstra, Jr., Primality testing, in Computational Methods in Number Theory, H. W. Lenstra, Jr. & R. Tijdeman, Amsterdam: Mathematisch Centrum (1984).
19. H.W. Lenstra, Jr., Primality testing algorithms [after Adleman, Rumely, and Williams], in Séminaire Bourbaki 576 (Lecture Notes in Mathematics #901), Springer (1981).
20. H.W. Lenstra, Jr., Finding isomorphisms between finite fields, Mathematics of Computation 56, pp. 329-347 (1991).
21. M. Mignotte and C.-P. Schnorr, Calcul déterministe des racines d'un polynôme dans un corps fini, Comptes Rendus Académie des Sciences (Paris) 306 (1988), 467-472.

22. J. Pila, Frobenius maps of Abelian varieties and finding roots of unity in finite fields, Mathematics of Computation 55, pp. 745-763 (1990).
23. S. Pohlig and M. Hellman, An improved algorithm for computing logarithms over GF(q) and its cryptographic significance, IEEE Transactions on Information Theory IT-24, pp. 106-110 (1978).
24. C. Pomerance and J. Sorenson, Counting the numbers cyclotomic methods can factor, J. Algorithms, submitted.
25. L. Rónyai, Factoring polynomials over finite fields, Proceedings of the 28th IEEE Symposium on Theory of Computing, pp. 132-137 (1987).
26. L. Rónyai, Factoring polynomials modulo special primes, Combinatorica 9, 199-206 (1989).
27. L. Rónyai, Galois groups and factoring polynomials over finite fields, Proceedings of the 30th IEEE Symposium on Theory of Computing, pp. 99-104 (1989).
28. R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Mathematics of Computation 44, pp. 483-494 (1985).
29. D. Shanks, Five Number-Theoretic Algorithms, Proceedings of the 2nd Manitoba Conference on Numerical Mathematics, pp. 51-70 (1972).
30. D. Shanks, Solved and Unsolved Problems in Number Theory (second edition), Chelsea (1972).
31. A. Tonelli, Bemerkung über die Auflösung quadratischer Congruenzen, Gottinger Nachrichten, 1891, pp. 344-46.
32. V. Shoup, On the deterministic complexity of factoring polynomials over finite fields, Information Processing Letters 33 (1990), 261-267.
33. B.L. van der Waerden, Modern Algebra (first English edition), Ungar (1949).