Deterministic Factorization of Polynomials over Special Finite Fields

Eric Bach

and

Joachim von zur Gathen

Computer Sciences Technical Report #799

October 1988

Deterministic Factorization of Polynomials over Special Finite Fields

Eric Bach
Computer Sciences Department
University of Wisconsin
Madison, WI 53706
USA

Joachim von zur Gathen
Computer Science Department
University of Toronto
Toronto, Ontario M5S 1A4
Canada

October 17, 1988

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 smallest prime factor of $p+1$. A similar result holds if we choose positive integers e and k and replace $p+1$ by $p^{ek}+\cdots+p^{e}+1$. Independently of any hypotheses, there is a deterministic polynomial time algorithm to factor polynomials mod p, when p is a Mersenne prime.

Submitted to *Mathematics of Computation*; available from UW-Madison Computer Sciences Department as Technical Report #799.

Sponsored by NSF [grants DCR-8504485 and DCR-8552596] and NSERC [grant 3-650-126-40].

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 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 [16] 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]. This result has been generalized in two directions. Taking a Galois-theoretic approach, Evdokimov [7] showed under the ERH that any polynomial in $\mathbb{Z}[X]$ with a solvable Galois group can be factored mod p in deterministic polynomial time; this extends results by Huang [9] and Adleman, Manders, & Miller [2]. Considering the number of factors, Ronyai [14] 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, the first fact to note is that only the characteristic matters, as Berlekamp [4] 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 [19] for the best current bounds on this time). One of the present authors [8] showed that if the ERH holds and $p - 1$ has only small prime factors – in this case we say that it is *smooth* – then polynomials can be factored modulo p by a deterministic polynomial time algorithm. Extensions of this result were found by Mignotte & Schnorr [12] and Ronyai [15].

In this paper we show that, assuming ERH, polynomials over fields of characteristic p such that $p + 1$ is smooth can be factored quickly; this answers a question posed in [8]. More generally, we show this to hold for fields such that for some fixed e and k, $p^{e(k-1)} + \cdots + p^e + 1$ is smooth (the dependence on k and e is not burdensome). Precise statements of our results can be found in the last theorems of sections of 4 and 5. Our results have the consequence that without any hypotheses, a deterministic polynomial time algorithm exists to factor polynomials modulo Mersenne primes.

This complements the known results on primality testing and integer factorization, to wit: smoothness of $\Phi_k(p)$, the kth cyclotomic polynomial evaluated at p, leads to fast algorithms to either prove p prime [11] or remove it as a factor from another number n [3]. The natural question to ask is if the smoothness of $\Phi_k(p)$ could help factor polynomials modulo p; this was also raised in [8] but we are presently unable to answer it.

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. For this reason we do not attempt to find the most efficient implementations of our methods. For practical purposes the randomized algorithms of Berlekamp [5] and Cantor & Zassenhaus [6] suffice to factor polynomials over any finite field.

The main features of our algorithm can be summarized as follows. Using standard techniques, we reduce the problem to that of factoring a polynomial modulo p. We then construct an extension field of the integers modulo p, together with elements that generate the kernel of the norm homomorphism. We need the ERH to show that this part is efficient, but it has to be done only once for a given prime. We then factor the polynomial over this extension field, using a process reminiscent of Pohlig & Hellman's algorithm [13] for computing indices; if the group of norm-1 elements has smooth order then this last part takes polynomial time.

Specifically, we use the ERH to get time bounds for solving the following problems: find an irreducible polynomial mod p, factor cyclotomic polynomials mod p, and construct an isomorphism between two realizations of a finite field.

The rest of this paper is organized as follows. Section 2 collects the algebraic results and notation that we need. All of the main ideas in our algorithm occur already when considering $p+1$; consequently we discuss this case in detail in sections 3 and 4. We present generalizations to other polynomials in p in section 5.

2. Notation and Background.

$\mathbb{F}_q$ 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. Although any two models of $\mathbb{F}_q$ are isomorphic, there is no known deterministic polynomial time algorithm to construct the isomorphism, although Evdokimov [7] has shown that the existence of such a method follows from the ERH.

The Galois group of $\mathbb{F}_{q^k}/\mathbb{F}_q$ is cyclic of order k and generated by the *Frobenius automorphism* $\sigma : x \to x^q$. 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 $x \rightarrow x^{m/m_i}$.

By the ERH we mean the following statement: the L-function attached to a Dirichlet character of a number field K has no zeroes in the half plane $Re(s) > 1/2$. This has the consequence that prime ideals that do not split in certain extensions of K can be found quickly; see [7] and [9] for more details on implications of the ERH.

For positive integers n, we let $S_k(n)$ denote the largest prime factor of $n^{k-1}+\cdots+1$; thus $S_2(p)$ is the largest prime factor of $p+1$.

3. Constructing Quadratic Extensions.

This section gives an algorithm to find a model of $\mathbb{F}_{p^2}$, together with an element outside the subgroup of rth powers for each prime r dividing $p+1$. 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 $p+1$.

Lemma 3.1. An isomorphism between any two given models of $\mathbb{F}_{p^2}$ can be found in deterministic polynomial time.

Proof. Using the quadratic formula we can assume the two models to be $K_i = \mathbb{F}_p(\sqrt{a_i})$, $i = 1, 2$. The a_i's must be quadratic nonresidues mod p. We use the Tonelli-Shanks algorithm [17] (which runs in deterministic polynomial time when given a quadratic nonresidue) to find a number $t \in \mathbb{F}_p$ with $t^2 = a_1/a_2$. An isomorphism between K_1 and K_2 is then given by $\sqrt{a_1} = t \cdot \sqrt{a_2}$. ■

Algorithm 3.2.

```
Input: $p$, an odd prime; $r$, a prime divisor of $p+1$.
Output: $K$, a model of $\mathbb{F}_{p^2}$; $\eta$, an element of $K - K^r$.
    Let $m = 2r$.
    Let $L = \mathbb{F}_p(\alpha)$ be a model of $\mathbb{F}_{p^m}$.
    Let $T$ denote the trace from $L$ to $\mathbb{F}_{p^2}$.
    Choose $i$, $0 \leq i < m$, so that $\tau = T(\alpha^i) \notin \mathbb{F}_p$.
    Let $K = \mathbb{F}_p(\tau)$.
    Let $\zeta$ be a root of $\Phi_r$; if $\zeta \notin \mathbb{F}_p$, adjoin $\zeta$ to $K$.
    Let $\beta = \alpha + \zeta\alpha^{p^2} + \ldots + \zeta^{r-1}\alpha^{p^{2(r-1)}}$.
    Return $K$ and $\eta = \beta^r$.
```

Theorem 3.3 [ERH]. Algorithm 3.2 correctly constructs K and η. It runs in time polynomial in r and $\log p$.

Proof. We first show correctness. The trace is an $\mathbb{F}_p$-linear mapping from L onto $\mathbb{F}_{p^2}$, hence one of the basis elements α^i will have its trace τ in $\mathbb{F}_{p^2}$ - $\mathbb{F}_p$. Since $r \mid p+1$, $\mathbb{F}_{p^2}$ must contain a primitive rth root of unity ζ. Now α generates $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^2}$, which is a cyclic extension whose degree r is relatively prime to p. β is the Lagrange resolvent, and by a classical theorem of algebra [20, §55], β^r is in $\mathbb{F}_{p^2}$ and β generates $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^2}$. It follows that η is in $\mathbb{F}_{p^2}$, 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 time bounded by a polynomial in m and $\log p$. The construction of K uses linear algebra to find the minimal polynomial for τ. Finally, we can factor Φ_r over $\mathbb{F}_p$ quickly under the ERH with the algorithm of Huang [9]. If Φ_r splits completely we take one of its roots as ζ, otherwise the factors must be of degree 2, and we use lemma 3.1 to express ζ in K. ■

Theorem 3.4 [ERH]. To construct a model of $\mathbb{F}_{p^2}$, together with a non-rth-power for every prime r dividing $p+1$, requires time polynomial in $S_2(p)$ and $\log p$.

Proof. Factor $p+1$, then run algorithm 3.2 using each prime r dividing $p+1$. Combine the models using lemma 3.1. ■

4. Factoring with Quadratic Extensions.

In this section we give an efficient algorithm to factor a polynomial over a finite field of characteristic p when $p+1$ is smooth. The algorithm requires a model of $\mathbb{F}_{p^2}$, together with certain generators for the norm-1 group of this field. First we need a purely algebraic result.

Lemma 4.1. Let K and L be fields, with $L = K(t)$. Let σ be a nontrivial automorphism of L fixing K. Define $\phi : \mathbb{F}_q \to K$ by $\phi(x) = (x+t)/(x+t^\sigma)$. Then ϕ is 1-1.

Proof: Choose x and y in K, and assume that $(x+t)/(x+t^\sigma) = (y+t)/(y+t^\sigma)$. Clear fractions, subtract common terms, and rearrange to find that $x(t-t^\sigma) = y(t-t^\sigma)$. Since t generates L/K, $t \neq t^\sigma$, so $x = y$. ∎

Using standard techniques, 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 [4, 5]. This latter problem is the one we shall actually solve.

Hence consider a polynomial $f \in \mathbb{F}_p[X]$ of degree l, with distinct roots in $\mathbb{F}_p$. We assume available a model of $\mathbb{F}_{p^2}$ as $\mathbb{F}_p(\tau)$, where τ satisfies an irreducible quadratic equation, together with non-rth-powers in $\mathbb{F}_{p^2}$ for each prime r dividing $p+1$. Our algorithm actually splits f in $\mathbb{F}_{p^2}[X]$; since f has all its roots in $\mathbb{F}_p$ any factor thus found must lie in $\mathbb{F}_p[X]$.

Algorithm 4.2.

Input: f, a polynomial in $\mathbb{F}_p[X]$ with distinct linear factors; $\mathbb{F}_p(\tau)$, a model of $\mathbb{F}_{p^2}$, and for each prime r dividing $p+1$, an element $\eta \in \mathbb{F}_p(\tau) - \mathbb{F}_p(\tau)^r$.

Output: A nontrivial factor of f.

```
Choose a nonconstant $u(X) \in \mathbb{F}_p[X]/(f(X))$.
Replace $u(X)$ by $u(X) + \tau$ (so now $u \in \mathbb{F}_{p^2}[X]$).
Let $d(X) = u(X)/u(X)^\sigma \bmod f(X)$ (if $u(X)$ is not a unit we immediately split $f(X)$).
For each prime $r$ dividing $p+1$:
    Find $s$ so that $r^s \,||\, p+1$.
    Let $\eta \notin \mathbb{F}_{p^2}^r$, and let $\gamma = \eta^{(p^2-1)/r^s}$, $\zeta = \gamma^{r^{s-1}}$.
    Set $v(X) = d(X)^{(p+1)/r^s} \bmod f(X)$.
    For $i = 0, \ldots, s-1$:
        Let $w(X) = v(X)^{r^{s-(i+1)}} \bmod f(X)$.
        If $w(X) \in \mathbb{F}_{p^2}$ (a constant) then:
            Find $e_i$ such that $\zeta^{e_i} = w(X)$.
            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 4.3. If $f \in \mathbb{F}_p[X]$ has distinct linear factors, then algorithm 4.2 finds a nontrivial factor of f. Its running time is bounded by a polynomial in $\log p$, $\deg f$, and $S_2(p)$.

Proof. The norm-1 group in $\mathbb{F}_{p^2}$ is isomorphic to $\prod_r C_{r^s}$, with the projection onto the rth factor given by $x \to x^{(p+1)/r^s}$. 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 factors of $f(X)$; for $i = 1, \ldots, l$, let d_i denote $d(X)$ modulo $f_i(X)$. Since $u(X)$ is not constant, applying the Chinese remainder theorem and lemma 4.1 (with the Frobenius automorphism of $\mathbb{F}_{p^2}/\mathbb{F}_p$) shows that two such d_i's, say d_1 and d_2, must be distinct. There is thus some r such that their projections v_1 and v_2 into C_{r^s} are distinct. 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 $0 \leq e_i < r$; choose the least i such that these "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 $e_i^{(1)} \neq e_i^{(2)}$. 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 4.4 [ERH]. Let $S_2(p)$ denote the largest prime factor of $p+1$. There is an algorithm with the following property: when presented with a polynomial $f \in \mathbb{F}_{p^k}[X]$ of degree n, it factors f in $O(kn \cdot S_2(p) \log p)^{O(1)}$ steps.

Proof. Combine theorem 4.3, the results of the last section, and the remarks on factoring polynomials over extension fields. ∎

A curious consequence of this is the following.

Corollary 4.4. There is a deterministic polynomial time algorithm that factors polynomials over $\mathbb{F}_p$, when p is a Mersenne prime (i.e., of the form $2^s - 1$ 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 [10]). 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 [18], p. 197).

5. Extensions.

In this section we discuss the modifications that must be done to replace $p+1$ by $q^{k-1}+\cdots+1$, when $q = p^e$. We shall present algorithms and theorems but merely sketch how the proofs should be changed. We first review Evdokimov's results:

Lemma 5.1 [ERH]. An isomorphism between any two given models of $\mathbb{F}_q$ can be found deterministically in time bounded by a polynomial in $\log q$. Furthermore, if $f \in \mathbb{Z}[X]$ is a polynomial with a solvable Galois group, then f can be factored over $\mathbb{F}_q$ in deterministic polynomial time.

Proof. See [7].

We next need an analog of theorem 3.3 to produce a model of $\mathbb{F}_{q^k}$ together with an non-rth-power for every prime r dividing $q^{k-1}+\cdots+q+1$. As before we can reduce this to the construction of a separate model for each r, and the algorithm to do this is given below.

Algorithm 5.2.

```
Input: $q$, an odd prime power; $r$, a prime divisor of $q^{k-1}+\cdots+q+1$.
Output: A model $K$ of $\mathbb{F}_{q^k}$ together with $\eta$, an non-$r$th-power.
    Let $m = kr$, and construct $L = \mathbb{F}_q(\alpha)$, a model of $\mathbb{F}_{q^m}$.
    Let $T$ denote the trace from $L$ to $\mathbb{F}_{q^k}$.
    Choose $i$, $0 \le i < m$, so that $\tau = T(\alpha^i)$ generates $\mathbb{F}_{q^k}/\mathbb{F}_q$.
    Let $K = \mathbb{F}_q(\tau)$.
    Let $\zeta$ be a root of $\Phi_r$; if $\zeta \notin \mathbb{F}_q$, adjoin $\zeta$ to $K$.
    Let $\beta = \alpha + \zeta\alpha^{q^k} + \cdots + \zeta^{r-1}\alpha^{q^{k(r-1)}}$.
    Let $\eta = \beta^r$.
```

Theorem 5.3 [ERH]. To construct a model of $\mathbb{F}_{q^k}$, together with a non-rth-power for every prime r dividing $q^{k-1}+\cdots+q+1$, requires time polynomial in k, $S_k(q)$ and $\log q$.

Proof. The proof goes through like that of theorem 3.4, provided that irreducible polynomials can be generated quickly and roots of unity found quickly in this relativized setting. As for the first problem, to construct an irreducible polynomial of degree m over $\mathbb{F}_q$, it suffices to construct an irreducible polynomial of degree em over $\mathbb{F}_p$ and then find an element α whose relative trace to $\mathbb{F}_q$ is contained in no smaller subfield. Then α will have degree m over $\mathbb{F}_q$, and using linear algebra we can find a relation between $1, \alpha, \ldots, \alpha^m$, which gives its minimal polynomial. Using lemma 5.1, we can identify this model of $\mathbb{F}_q$ with any given one. As for the second problem, if r is prime then the r-th cyclotomic polynomial has a cyclic Galois group, so lemma 5.1 certainly applies. ∎

Algorithm 5.4.

Input: f, a polynomial in $\mathbb{F}_q[X]$ with distinct linear factors; $\mathbb{F}_q(\tau)$, a model of $\mathbb{F}_{q^k}$ together with a non-rth-power η for each prime divisor r of $q^{k-1} + \cdots + q + 1$.

Output: A nontrivial factor of f.

```
Choose a nonconstant $u(X) \in \mathbb{F}_q[X]/(f(X))$.
Replace $u(X)$ by $u(X) + \tau$.
Let $d(X) = u(X)/u(X)^\sigma \bmod f(X)$.
For each prime $r$ dividing $q^{k-1} + \cdots + q + 1$:
    Find $s$ so that $r^s \,||\, q^{k-1} + \cdots + q + 1$.
    Let $\eta \notin \mathbb{F}_{q^k}^r$, and let $\gamma = \eta^{(q^k-1)/r^s}$, $\zeta = \eta^{r^{s-1}}$.
    Set $v(X) = d(X)^{(q^{k-1}+\cdots+q+1)/r^s} \bmod f(X)$.
    For $i = 0, \ldots, s-1$:
        Let $w(X) = v(X)^{r^{s-(i+1)}} \bmod f(X)$.
        If $w(X) \in \mathbb{F}_{q^k})$, then find $e_i$ such that $\zeta^{e_i} = w(X)$ and replace $v(X)$ by $v(X)/\gamma^{e_i r^i}$.
        Otherwise, find $j$, $0 \le j < r$, such that $\gcd(v - \zeta^j, f)$ splits $f$.
```

Theorem 5.5. Algorithm 5.4 splits f, in time polynomial in k, $\log q$, $\deg f$, and $S_k(q)$.

Proof. Like that of theorem 4.3; left to the reader. ■

Theorem 5.6 [ERH]. Let $S_k(m)$ denote the largest prime factor of $m^{k-1} + \cdots + m + 1$. There is an algorithm with the following property: when given positive integers k and e, it factors any degree n polynomial over a finite field F of characteristic p in $O(ke \cdot nS_k(p^e) \log |F|)^{O(1)}$ steps.

Proof. Reduce the problem to that of factoring a squarefree polynomial f into distinct linear factors over $\mathbb{F}_p$. Then construct a field with $q = p^e$ elements using the algorithm of [1], and use algorithms 5.2 and 5.4 to factor f over $\mathbb{F}_q$. ■

Acknowledgements. Much of this work was done during a visit by the first author to the University of Toronto; we wish to thank the Information Technology Research Centre, Province of Ontario, for sponsoring this visit. 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. E. Bach and J. Shallit, Factoring with cyclotomic polynomials, to appear, Mathematics of Computation, January 1989. [Preliminary version in 1985 FOCS.]

4. E.R. Berlekamp, Factoring polynomials over finite fields, Bell System Technical Journal 46 (1967), pp. 1853-1859.

5. E.R. Berlekamp, Factoring polynomials over large finite fields, Mathematics of Computation 24 (1970), pp. 713-735.

6. D. Cantor and H. Zassenhaus, Factoring polynomials over finite fields, Mathematics of Computation 36, pp. 587-592 (1981).

7. S.A. Evdokimov, Efficient factorization of polynomials over finite fields and generalized Riemann hypothesis, preprint, Leningrad Institute for Informatics and Automatization (1988).

8. J. von zur Gathen, Factoring polynomials and primitive elements for special primes, Theoretical Computer Science 52, pp. 77-89 (1987).

9. 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).

10. H.W. Lenstra, Jr., Primality testing, in Computational Methods in Number Theory [ed. Lenstra & Tijdeman], Amsterdam: Mathematisch Centrum (1984).

11. H.W. Lenstra, Jr., Primality testing algorithms [after Adleman, Rumley, and Williams], in Sèminaire Bourbaki 576 (Lecture Notes in Mathematics #901), Springer (1981).

12. M. Mignotte and C.-P. Schnorr, to appear.

13. 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).

14. L. Ronyai, Factoring polynomials over finite fields, Proceedings of the 28th IEEE Symposium on Theory of Computing, pp. 132-137 (1987).

15. L. Ronyai, Factoring polynomials modulo special primes, to appear, Combinatorica.

16. R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Mathematics of Computation 44, pp. 483-494 (1985).

17. D. Shanks, Five Number-Theoretic Algorithms, Proceedings of the 2nd Manitoba Conference on Numerical Mathematics, pp. 51-70 (1972).

18. D. Shanks, Solved and Unsolved Problems in Number Theory (second edition), Chelsea (1972).

19. V. Shoup, On the deterministic complexity of factoring polynomials over finite fields, Computer Sciences Technical Report #782, University of Wisconsin (1988).

20. B.L. van der Waerden, Modern Algebra (first English edition), Ungar (1949).