Finding Irreducible Polynomials over Finite Fields

Conference Paper · November 1986

DOI: 10.1145/12130.12166 · Source: DBLP

2 authors, including:

Hendrik Lenstra
Leiden University
70 PUBLICATIONS **1,839** CITATIONS

SEE PROFILE

FINDING IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

Leonard M. Adleman[1]
Dept. of Computer Science
University of Southern California

Hendrik W. Lenstra, Jr.
Mathematisch Instituut
Universiteit van Amsterdam
and Mathematical Sciences Research Institute

I. Introduction

Irreducible polynomials in $\mathbf{F}_p[x]$ are used to carry out the arithmetic in field extension of $\mathbf{F}_p$. Computations in such extensions occur in coding theory [2], complexity theory [8] and cryptography [3]. Random polynomial time algorithms exist for finding irreducible polynomials of any degree over $\mathbf{F}_p$ [2, 8], and so as a practical matter the problem is solved. However, the deterministic complexity of the problem has yet to be established.

We present two results:

Theorem 1: There is a $c \in \mathbf{Z}_{>0}$ and an algorithm A such that on input $p,d \in \mathbf{Z}_{>1}$ with p prime:

1. Outputs $f \in \mathbf{F}_p[x]$ with f irreducible and $dg(f)=d$.

2. Assuming extended Riemann hypothesis, halts within $(d \log p)^c$ steps.

Theorem 2: There is a $c \in \mathbf{Z}_{>0}$ and an algorithm B such that on input $p,d \in \mathbf{Z}_{>1}$ with p prime:

1. Outputs $f \in \mathbf{F}_p[x]$ with f irreducible and $d/c \log p < dg(f) \leq d$.

2. Halts within $(d \log p)^c$ steps.

II. Notation

If K is a field $\overline{K}$ will denote an algebraic closure. When p is a rational prime, $\mathbf{F}_p$ will denote the field with p elements. If K is a number field (i.e. finite extension of Q) O_K will denote its ring of integers. When a rational prime p and a number field K are fixed, then for $\alpha \in O_K$, $\bar{\alpha}$ will denote $\alpha+pO_K$. If a rational prime p is fixed, then for $f \in \mathbf{Z}[x]$, $f = \sum_{i=0}^{d} a_i x^i$, $\bar{f}$ will denote $\sum_{i=0}^{d} \bar{a}_i x^i \in \mathbf{F}_p[x]$. For $n \in \mathbf{Z}_{>1}$, ζ_n will denote $e^{\frac{2\pi i}{n}}$

III. Algorithm A

(0) Input $p,d \in \mathbf{Z}_{>1}$

(1) Calculate $n,a \in \mathbf{Z}_{>0}$ such that:
$d = p^a n$ with $(p,n) = 1$.

(2) Calculate $q \in \mathbf{Z}_{>0}$ such that:
q is the least prime with $q \equiv 1 \pmod{n}$
and p inert in the subfield $K \subseteq Q(\zeta_q)$
with $[K:Q] = n$.

(3) Calculate $g \in \mathbf{F}_p[x]$ such that:

$$g = \overline{\prod_{\sigma \in G_{K/Q}} (x - \eta^\sigma)}$$

where $\eta = \mathrm{Tr}_{Q(\zeta_q)/K}(\zeta_q)$.

[1]Research sponsored by NSF Grant No. MCS-8022533

(4) For i = 1,2,...,d calculate $a_{i,1},a_{i,2},...,a_{i,d} \in \mathbf{F}_p$ such that:

$V_i(\beta+\alpha_a) = \sum_{j=1}^{d} a_{i,j}V_j$ where

$V_i = \beta^e \prod_{\ell=1}^{a} \alpha_\ell^{e_\ell} \in \overline{\mathbf{F}}_p$ for

$i \equiv \sum_{\ell=1}^{a} e_\ell p^{\ell-1} \pmod{p^a}$ with $e_\ell \in \{0,1,..,p-1\}$ for $\ell=1,2,...,a$.

$i \equiv e \pmod{n}$ with $e \in \{0,1,...,n-1\}$.

$\alpha_1 \in \overline{\mathbf{F}}_p$ is a root of $f_1 = x^p-x-1 \in \mathbf{F}_p[x]$

$\alpha_\ell \in \overline{\mathbf{F}}_p$ is a root of $f_\ell = x^p-x-[\prod_{j=1}^{\ell-1} \alpha_j]^{p-1} \in \mathbf{F}_p(\alpha_1,\alpha_2,...,\alpha_{\ell-1})[x]$ for $\ell = 2,3,...,a$

$\beta \in \overline{\mathbf{F}}_p$ is a root of g

(5) Calculate $f \in \mathbf{F}_p[x]$ such that f is the characteristic polynomial of $(a_{i,j}) \in M_d(\mathbf{F}_p)$.

(6) Output f*.

IV. Proof of Correctness-Algorithm A

We begin by arguing that Algorithm A runs in polynomial time assuming extended Riemann hypothesis.

Step (1) clearly is polynomial time. For Step (2) we used a varient of Theorem 2 in [1].

Proposition 3: Assuming extended Riemann hypothesis, there is a $c \in \mathbf{Z}_{>0}$ such that for all $p,n \in \mathbf{Z}_{>0}$ with p prime and (p,n) = 1 there is a prime $q \equiv 1 \pmod{n}$ with $q < cn^4(\log(np))^2$ such that p is inert in the (unique) subfield $K \subseteq Q(\zeta_q)$ with [K:Q] = n.

Hence the q required in Step (2) is sufficiently small that it can be found and tested for primality in polynomial time. Since p is inert in K iff $(q-1/f,n) = 1$ where f is the order of p in $(\mathbf{Z}/\ q\mathbf{Z})^*$ this too can be tested in polynomial time.

For Step (3) we begin by noting that it follows from Gauss' theory of periods (see [9]) that $\prod_{\sigma \in G_{K/Q}} (x-\eta^\sigma) \in \mathbf{Z}[x]$ so the definition of g makes sense. Since $\overline{\prod_{\sigma \in G_{K/Q}} (x-\eta^\sigma)} = \prod_{\sigma \in G_{K/Q}} (x-\overline{\eta^\sigma})$, the calculation of g can be done using the ring operations in $\mathbf{Z}[\zeta_q]/p\mathbf{Z}[\zeta_q]$ which are polynomial in q log p. It follows that Step (3) can be done in polynomial time.

For Step (4) it suffices to show that for a fixed i the calculation of the $a_{i,j}$'s takes polynomial time. The calculation proceeds in a+1 stages. In Stage 1 powers of β greater than n-1 are reduced using g. In stage i = 2,3,...,a+1 powers of α_{a+2-i} greater than p-1 are reduced using f_{a+2-i}. The remaining details are straightforward.

The calculation of the characteristic polynomial of a matrix of $M_d(\mathbf{F}_p)$ can be done in time polynomial in d log p using standard methods [10, pp. 353-355, 410-411].

We now argue that the polynomial $f \in \mathbf{F}_p[x]$ produced by Algorithm A is irreducible of degree d. We begin by considering the following tower of fields:

$$\begin{array}{ccccccccccc} F_0 & - & F_1 & - & F_2 & - \cdots - & F_{a-1} & - & F_a & - & F & - & \overline{F}_p \\ \| & & \| & & \| & & \| & & \| & & \| & & \\ F_p & & F_0(\alpha_1) & & F_1(\alpha_2) & & F_{a-2}(\alpha_{a-1}) & & F_{a-1}(\alpha_a) & & F_a(\beta) & & \end{array}$$

Where $\alpha_1, \alpha_2, ..., \alpha_a, \beta$ are as in the algorithm.

We will prove the following claims:

Claim I $[F_i : F_{i-1}] = p$ for i = 1,2,...,a

Claim II $[F : F_a] = n$

Claim III $F = \mathbf{F}_p(\beta+\alpha_a)$

It follows from the claims that $\beta+\alpha_a$ satisfies a unique d^{th} degree monic irreducible polynomial in $\mathbf{F}_p[x]$. Since the V_i of the Algorithm are clearly a basis for $F/\mathbf{F}_p$ it follows from standard result (see for example [7], pages 7-8) that f is the desired polynomial.

Claim I will follow from the next two lemmas, variants of which may be found in [7] for example:

Lemma 4: Let K be a field of characteristic $p \neq 0$ and $a \in K$. Then either $f = x^p-x-a$ is irreducible or it has a root in K.

Proof: If $\alpha,\beta \in \overline{K}$ are roots of f then $(\alpha-\beta)^p = \alpha-\beta$, so $\alpha-\beta \in \mathbf{F}_p$. Therefore $K(\alpha) = K(\beta)$, and α and β have the same degree over K. It follows that all irreducible factors of f in K[x] have the same degree. But f has prime degree, so either f is irreducible or all its factors are linear. □

Lemma 5: Let K be a field of characteristic $p \neq 0$, $a \in K$ with $f = x^p-x-a \in K[x]$ irreducible, $\alpha \in \overline{K}$ a root of f. Then $g = x^p-x-a\alpha^{p-1} \in K(\alpha)[x]$ is irreducible.

Proof: Let Tr denote the trace function from $K(\alpha)$ to K. We will calculate $Tr(\alpha^{p-1})$. By assumption,

(*) $\quad \alpha^p-\alpha-a \equiv 0$

Multiplying (*) by α^{-1} gives $\alpha^{p-1} = a\alpha^{-1}+1$ so $Tr(\alpha^{p-1}) = Tr(a\alpha^{-1}+1) = aTr(\alpha^{-1})+Tr(1) = aTr(\alpha^{-1})$. Multiplying (*) by $(\alpha^{-1})^p a^{-1}$ gives $a^{-1}-(a^{-1})(\alpha^{-1})^{p-1}-(\alpha^{-1})^p = 0$ from which it follows that $-a^{-1}+a^{-1}x^{p-1}+x^p$ is the monic irreducible polynomial for α^{-1} and $Tr(\alpha^{-1}) = -a^{-1}$. Hence $Tr(\alpha^{p-1}) = -1$.

Assume g is reducible then by Lemma 4 there is a $\beta \in K(\alpha)$ with $\beta^p-\beta-a\alpha^{p-1} = 0$. Taking traces (and observing that raising to the p^{th} power commutes with taking trace) yields $b^p-b-a = 0$ for $b = -Tr(\beta) \in K$ contradicting the hypothesis that $f \in K[x]$ is irreducible. □

By Lemma 4, $f_1 = x^p-x-1 \in \mathbf{F}_p[x]$ is either irreducible or has a root in $\mathbf{F}_p$. In the latter case, $(x^p-x-1, x^p-x) \neq 1$, which is clearly not correct. Thus $[F_1:F_0] = p$. The rest of Claim I now follows from Lemma 5.

Claim II follows from the next lemma which is basically due to Kummer [5].

Lemma 6: Let $p,q,n \in \mathbf{Z}_{>0}$ with p,q prime, $q \equiv 1 \pmod{n}$ and p inert in the subfield $K \subseteq Q(\zeta_q)$ with $[K:Q] = n$. Let

$$g = \overline{\prod_{\sigma \in G_{K/Q}} (x-\eta^\sigma)}$$

where $\eta = Tr_{Q(\zeta_q)/K}(\zeta_q)$, then g is irreducible in $\mathbf{F}_p[x]$.

Proof: It is well known [9] that $S = \{\eta^\sigma : \sigma \in G_{K/Q}\}$ is a basis for O_K over $\mathbf{Z}$. Hence $\overline{S} = \{\overline{\eta^\sigma} : \sigma \in G_{K/Q}\}$ is a basis for the n^{th} degree extension field O_K/pO_K as a vector space over $\mathbf{F}_p$. It follows that $\overline{S}$ has n elements. The field automorphisms of O_K/pO_K induced by the elements of $G_{K/Q}$ permute $\overline{S}$ transitively. Hence the elements of $\overline{S}$ are conjugate over $\mathbf{F}_p$. It follows that g is irreducible in $\mathbf{F}_p[x]$. □

Notice that since f_a is irreducible in $\mathbf{F}_p(\alpha_1,\alpha_2,\ldots,\alpha_{a-1})[x]$ it follows that $F_a = \mathbf{F}_p(\alpha_a)$. Now Claim III follows from:

Lemma 7: Let $\alpha,\beta \in \overline{\mathbf{F}}_p$ with $[\mathbf{F}_p(\alpha):\mathbf{F}_p]$ and $[\mathbf{F}_p(\beta):\mathbf{F}_p]$ relatively prime. Then $\mathbf{F}_p(\alpha,\beta) = \mathbf{F}_p(\alpha+\beta)$.

Proof: Let $d_\alpha = [\mathbf{F}_p(\alpha):\mathbf{F}_p]$, $d_\beta = [\mathbf{F}_p(\beta):\mathbf{F}_p]$, $d_{\alpha+\beta} = [\mathbf{F}_p(\alpha+\beta):\mathbf{F}_p]$. Since $\mathbf{F}_p \subseteq \mathbf{F}_p(\alpha) \subseteq \mathbf{F}_p(\beta,\alpha+\beta)$ we have $d_\alpha | [\mathbf{F}_p(\beta,\alpha+\beta):\mathbf{F}_p]$. Also $[\mathbf{F}_p(\beta,\alpha+\beta):\mathbf{F}_p] | d_\beta d_{\alpha+\beta}$ so $d_\alpha | d_\beta d_{\alpha+\beta}$. Similarly $d_\beta | d_{\alpha+\beta}$ hence $d_\alpha d_\beta | d_{\alpha+\beta}$. Clearly $\mathbf{F}_p(\alpha+\beta) \subseteq \mathbf{F}_p(\alpha,\beta)$ so they must be equal. □

Remark: Assume the extended Riemann hypothesis, then the polynomial f that is calculated by Algorithm A has "small coefficients," if α is small and p is large. More precisely, f is of the form $f = x^d+\sum_{i=1}^{d} \bar{a}_i x^{d-i}$, where $\alpha_i \in \mathbf{Z}$ satisfies

$$|a_i| \leq c^i d^{4i} (log(dp))^{2i}, \text{ for } i = 1,2,\ldots,d,$$

with c as in Proposition 3.

Without the extended Riemann hypothesis it is not clear how to prove the existence of an irreducible polynomial in $\mathbf{F}_p[x]$ of this form.

V. Algorithm B

(0) Input $p,d \in \mathbf{Z}_{>1}$

(1) Set $c_0 = a_0 = b_0 = 1$, set $g_0 = x-1 \in \mathbf{F}_p[x]$.

(2) For $i = 1,2,...,z$ calculate $<q_i,a_i,b_i,c_i,g_i>$ such that:

q_i = least positive prime with q_i-1 square free,

$q_i \neq p$ and $q_i \nmid p^{c_{i-1}}-1$

a_i = least positive integer with $p^{a_i} \equiv 1 \bmod q_i$

$b_i = a_i/(a_i,c_{i-1})$

$c_i = b_i c_{i-1}$

$g_i \in \mathbf{F}_p[x]$ such that $g_i(x) = \prod_{\sigma \in G_{K/Q}} (x-\eta^\sigma)$

where

K is the unique subfield of $Q(\zeta_{q_i})$

with $[K:Q] = b_i$

$\eta = \mathrm{Tr}_{Q(\zeta_{q_i})/K}(\zeta_{q_i})$

z = least positive integer such that $c_z \geq d$

(3) Calculate $I \subseteq \{0,1,...,z\}$ as follows:

Set $t_z = 1$.

For $j = z,z-1,...,1$

(a) If $t_j b_j \leq d$ then set $t_{j-1} = t_j b_j$, put $j \in I$.

(b) If $t_j b_j > d$ and $t_j c_{j-1} < d$ then set $t_0 = t_j c_{j-1}$, put $0,1,...,j-1 \in I$, goto (4)

(c) If $t_j b_j > d$ and $t_j c_{j-1} \geq d$ then set $t_{j-1} = t_j$.

(4) For $i = 1,2,...,t_0$ calculate $a_{i,1},a_{i,2},...,a_{i,t_0} \in \mathbf{F}_p$ such that:

$V_i\gamma = \sum_{j=1}^{t_0} a_{i,j}V_j$ where

$V_i = \prod_{k \in I} \beta_k^{e_k} \in \overline{\mathbf{F}}_p$ for

$i \equiv e_k \pmod{b_k}$ with $e_k \in \{0,1,...,b_{k-1}\}$ for $k \in I$.

$\beta_k \in \overline{\mathbf{F}}_p$ is a root of $g_k \in \mathbf{F}_p[x]$ for $k \in I$.

$\gamma = \sum_{k \in I} \beta_k \in \overline{\mathbf{F}}_p$.

(5) Calculate $f \in \mathbf{F}_p[x]$ such that:

f is characteristic polynomial of $(a_{ij}) \in M_{t_0}(\mathbf{F}_p)$.

(6) Output f^*.

VI. Proof of Correctness - Algorithm B

We begin by proving the following claim (the notation is that of Algorithm B):

Claim IV: There exists a $c \in \mathbf{Z}_{>0}$ such that for all $p,d \in \mathbf{Z}_{>1}$ with p prime, the b_i's and q_i's produced in Algorithm B on inputs p,d have the following properties:

(a) $2 \leq b_i < q_i \leq cc_{i-1} \log p < cd\log p$ $i = 1,2,...,z$.

(b) $(b_i,b_j) = 1$ for $1 \leq i < j \leq z$.

We will need the following well known result, which is a direct consequence of Theorem 2 in [6] (put $k = 2$ and $\ell = -1$):

Proposition 8: There exists a $c \in \mathbf{Z}_{>0}$ such that for all $p,x \in \mathbf{Z}$ with p prime and $x \geq 3$

$$\prod_{\substack{q \leq x \\ q \text{ prime} \\ q-1 \text{ square free} \\ q \neq p}} q > e^{x/c}$$

Proof of Claim IV: Clearly $1 \leq b_i \leq a_i$. Assume $b_i = 1$, then $a_i | c_{i-1}$ so $p^{c_{i-1}} \equiv 1 \bmod q_i$ and contrary to our construction $q_i | p^{c_{i-1}}-1$. By Fermat's Little Theorem $a_i \leq q_i-1 < q_i$ so $b_i < q_i$. By Proposition 8

$$\prod_{\substack{q \leq cc_{i-1}\log p \\ q \text{ prime} \\ q-1 \text{ square free} \\ q \neq p}} q > p^{c_{i-1}} > p^{c_{i-1}}-1$$

so $q_i \leq cc_{i-1} \log p$ as claimed. $cc_{i-1}\log p < cd\log p$ for $i = 1,2,...,z$ by the choice of z in Step (2). Therefore (a) holds. (b) Is clear from the construction. □

It follows from (a) of Claim IV that $z \leq \log d$ and that each q_i can be found in polynomial time by naive search. Step (2) is now easily seen to be computable in polynomial time. The other steps are proved to be

computable in polynomial time using simple varients of the arguments used for Algorithm A.

It is clear from the construction, (b) of Claim IV, and the arguments for Algorithm A that the output f of Algorithm B is irreducible of degree t_0. (Note in particular that p is inert in each of the fields K occurring in Step (2), because the square-freeness of q_i-1 implies that $((q_i-1)/a_i,b_i)=1$).

Consider Step (3) of the algorithm. At the start we have $t_z c_z = c_z \geq d$. Assume that at stage j we have $t_j c_j \geq d$, then if option (a) is executed we have $t_{j-1}c_{j-1} = t_j b_j c_{j-1} = t_j c_j \geq d$. If option (c) is executed we have $t_{j-1}c_{j-1} = t_j c_{j-1} \geq d$. It follows that if option (b) is never executed then $t_0 = t_0 c_0 \geq d$. On the other hand, if for some j option (b) is executed then using (a) of claim IV we get $d < t_j b_j < t_j\, cc_{j-1} \log p = t_0\, c \log p$ so $t_0 > d/c \log p$. In any case, since it is clear from Step (3) that we always have $t_0 \leq d$, we get

$$\frac{d}{c \log p} < t_0 \leq d$$

as desired.

VII. Conclusion

A deterministic algorithm for finding an irreducible polynomial of desired degree in $\mathbf{F}_p[x]$ is presented. The algorithm runs in polynomial time if an extension of Riemann hypothesis is assumed. A second algorithm which runs in deterministic polynomial time without hypothesis and produces an irreducible polynomial of approximately the desired degree is also presented.

The obvious remaining problems are to remove the need for extended Riemann hypothesis in Algorithm A or substantially improve the approximation achieved in Algorithm B. These both may be difficult since the solution to either would imply the solution to other well known problems in number theoretic computational complexity. For example, removal of the need for extended Riemann hypothesis in Algorithm A, would provide a means of finding irreducible quadratic polynomials, which in turn would provide a deterministic polynomial time algorithm for finding quadratic nonresidues and taking square roots in $\mathbf{F}_p$.

VIII. Acknowledgments

We would like to thank J. Von zur Gathen for bringing this problem to our attention. For additional results on this problem see Von zur Gathen [4].

References

[1] E. Bach and J. Shallit, "Factoring with Cyclotomic Polynomials," Proceedings 26th FOCS, 1985, pp. 443-450.

[2] E.R. Berlekamp, "Algebraic Coding Theory," McGraw-Hill Publishing Company, New York, 1968.

[3] B. Chor and R. Rivest, "A Knapsack Type Public Key Cryptosystem Based on Arithmetic in Finite Fields," Advances in Cryptography (Ed., G. Goos and J. Hartmanis), Springer-Verlag, New York, pp. 54-65.

[4] J. Von zur Gathen, "Irreducible Polynomials Over Finite Fields," Manuscript, 1985.

[5] E.E. Kummer, Uber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen, J. reine angew. Math. 30 (1846), 107-116; pp. 193-202 in Collected papers, Springer-Verlag, Berlin, 1975.

[6] L. Mirsky, "The Number of Representations of an Integer as the Sum of a Prime and a k-free Integer," Amer. Math. Monthly 56 (1949), 17-19.

[7] P.J. McCarthy, "Algebraic Extensions of Fields," Blaisdell Publishing Company, Waltham, Mass., 1966

[8] M.O. Rabin, "Probabilistic Algorithms in Finite Fields," SIAM J. Comput., Vol. 9, (1980), pp. 273-280.

[9] L. Washington, "Cyclotomic Fields," Springer-Verlag, New York 1980.

[10] J.H. Wilkinson, "The Algebraic Eigenvalue Problem," Oxford Clarendon Press, 1965, pp. 353-355 and 410.