Factoring Polynomials in $\mathbb{F}_p[X]$

Andrei Jorza

March 1, 2005

1 Generalities

We will denote by I_n the set of irreducible (monic) polynomials of degree n in $\mathbb{F}_p[X]$. There are a few questions. Is I_n nonempty? Can one test whether $f \in I_n$? Is there is fast algorithm to decompose a (random) polynomial in $\mathbb{F}_p[X]$ into irreducible factors?

Proposition 1.1. *Let $f \in \mathbb{F}_p[X]$ be an irreducible polynomials of degree n. Then $f(X) \mid X^{p^n} - X$ and $f(X) \nmid X^{p^m} - X$ for any $m < n$.*

Proof. We can realize $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(f)$ so f has a root in $\mathbb{F}_{p^n}$, which in turn is a root of $X^{p^n} - X$. Therefore $(f(X), X^{p^n} - X) \neq 1$ in $\mathbb{F}_{p^n}[X]$ and so in $\mathbb{F}_p[X]$. Since $f(X)$ is irreducible over $\mathbb{F}_p[X]$ this implies that $f(X) \mid X^{p^n} - X$.

Assume that $f(X) \mid X^{p^m} - X$ for some m. Then f has a root α in $\mathbb{F}_{p^m}$, since $\mathbb{F}_{p^m}$ is the set of roots of $X^{p^m} - X$. Then $1, \alpha, \ldots, \alpha^m$ are $m+1$ vectors in the m-dimensional vector space $\mathbb{F}_{p^m}/\mathbb{F}_p$. Therefore they are linearly dependent. Therefore the minimal polynomial $g(X)$ of α in $\mathbb{F}_p[X]$ will have degree $m < n$, which contradicts the fact that $f(X)$ is irreducible. □

Theorem 1.2. *Let $n \geq 2$ be a positive integer. Then*

$$X^{p^n} - X = \prod_{d \mid n} \prod_{f \in I_d} f.$$

Proof. For every $d \mid n$ and every $f \in I_d$ we know that $f(X) \mid X^{p^d} - X \mid X^{p^m} - X$ (because $X^{p^n} - X$ is Mersenne). Since all the polynomials f are irreducible so coprime, their product will divide $X^{p^n} - X$. □

Corollary 1.3. *Let $a_n = |I_n|$. Then*

$$a_n \geq \frac{p^n - (\log n) p^{n/2}}{n}.$$

Proof. By degree comparison, Theorem 1.2 gives $p^n = \sum_{d|n} d a_d$. By the Möbius inversion formula we get that

$$a_n = \frac{1}{n} \sum_{d|n} p^d \mu(n/d).$$

If $n = p_1^{n_1} \cdots p_k^{n_k}$ then $a_n \geq \frac{1}{n}(p^n - \sum_1^k p^{n/p_i}) \geq \frac{1}{n}(p^n - kp^{n/2})$. □

In conclusion I_n is nonempty for all $n \geq 2$.

2 Irreducibility Testing

2.1 Theory

Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree n. We would like to devise a test to see if $f \in I_n$. We have seen that if f is irreducible then $f(X) | X^{p^n} - X$ and for all $m < n$ $(f(X), X^{p^m} - X) = 1$. Evidently, a counterexample to this would have $m|n$ so it is enough to check this condition for $m = n/p_i$ for each prime divisor p_i of n. Let's make things formal

Theorem 2.1. *$f \in I_n$ if and only if*

1. *$f(X) | X^{p^n} - X$.*

2. *For each $p_i \mid n$ a prime divisor we have $(f(X), X^{p^m} - X) = 1$ for $m = n/p_i$.*

Proof. Assume that f is irreducible. Then f will pass the test by what we have already seen. Assume that $f = f_1^{\ell_1} \cdots f_r^{\ell_r}$. If $\ell_j > 1$, then $f_i^2 \mid f$ cannot divide $X^{p^n} - X$ since this polynomial is a product of distinct irreducible polynomials. So $\ell_i = 1$ for all i.

Let α be a root of f_1. If $r \neq 1$ then $\deg f_1 < n$ so α has degree $< n$ over $\mathbb{F}_p$. Moreover, if f passes test 1 then $\alpha \in \mathbb{F}_{p^n}$ so $\mathbb{F}_{p^n}/\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is a field extension tower. Therefore $\deg \alpha \mid n$ so $\deg \alpha \mid n/p_i$ for some i. Then $f_1 \mid X^{p^{n/p_i}} - X$ so test 2 fails. □

2.2 Running Time

The first test is $X^{p^n} \equiv X \pmod{f(X)}$ and this can be done in $n \log p$ steps using repeated squarings. The second test needs $\log n$ tests of the form $\gcd(f(X), X^{p^m} - X) = 1$. Each such test uses the Euclidean algorithm that needs m operations with degree $\leq m$ polynomials. So the running time of each such Euclidean algorithms is roughly $\mathcal{O}(n^3)$, although it might be faster in practice.

3 Finding Roots $\pmod{p}$

Let $p \neq 2$ be a prime number. Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree m, and we may assume that 0 is not a root. We want to find a root of f in $E = \mathbb{F}_{p^n}$. Let $q = p^n$. If $(f(X), X^{q-1} - 1) = 1$ then f clearly has no roots in E. Otherwise, let $f_0(X) = \gcd(f(X), X^{q-1} - 1)$, and all the roots of f in E will be roots of f_0. Write $f_0(X) = (X - a_1) \cdots (X - a_k)$. Whether all the roots are equal it is easy to check: simply compute all the derivatives of f and each should divide f. Assume that not all the roots are equal.

Lemma 3.1. *Let $u \neq v \in E$. The the number of $w \in E$ such that one of the following two cases is satisfied is $(q-1)/2$:*

1. *$u + w$ is a root of $X^{(q-1)/2} - 1$ and $v + w$ is a root of $X^{(q-1)/2} + 1$.*
2. *$u + w$ is a root of $X^{(q-1)/2} + 1$ and $v + w$ is a root of $X^{(q-1)/2} - 1$.*

Proof. For such a w it is clear that $(u + w)/(v + w)$ is a quadratic nonresidue mod q, of which there are $(q - 1)/2$. Moreover, for every quadratic nonresidue c there is a unique w such that $(u + w)/(v + w) = c$ since $u \neq v$. $\square$

For $d \in E$ write $f_d(X) = f_0(X - d)$. Then the roots of f_d are $a_1 + d, \ldots, a_k + d$ and by the lemma above for half of the d's, there exist i, j such that $a_i \neq a_j$ and d satisfies the conditions in the lemma.

Proposition 3.2. *If d satisfies the conditions in the lemma for a_i, a_j then $\gcd(f_d(X), X^{(q-1)/2} - 1) = h_d(X)$ has degree $< \deg f_d(X)$.*

Proof. Otherwise $f_d(X) \mid X^{(q-1)/2} - 1$ so all the roots are quadratic residues which contradicts the assumption on d. $\square$

Algorithm 3.3.

Input f.

Compute $f_0(X) = \gcd(f(X), X^{q-1} - 1)$.

Choose $d \in E$ randomly.

Compute $\gcd(f_d(X), X^{(q-1)/2} - 1) = h_d(X)$. With probability 1/2 we have $\deg h_d(X) < \deg f_d(X)$. Repeat until this happens.

Then $h_d(X) \mid f_d(X)$ so $h_d(X+d) \mid f_0(X)$ is a proper factor.

Repeat the algorithm for $h_d(X+d)$ until reach a linear factor.

Output a root of the last linear factor which will be a root of $f(X)$ in E.

Problem 3.4. For a prime $p \equiv 1 \pmod 4$ find a, b integers so that $p = a^2 + b^2$.

Proof. Let u be a root of $X^2 + 1 \pmod p$, found as above. Then you know that $(a+bi) \mid (u+i)$ so use the Euclidean algorithm in $\mathbb{Z}[i]$ to find $a+bi = \gcd(p, u+i)$. $\square$

4 Factorisation $\pmod p$

4.1 Theory

Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree n. We would like to factor f into irreducible polynomials in $\mathbb{F}_p[X]$. Test to see if irreducible, stop if yes. Otherwise continue.

For each $k \in \{1, \ldots, n\}$ find $h_k(X) = \gcd(f(X), X^{p^k-1} - 1)$. For each $h_k \neq 1$ we have $h_k(X) | f(X)$ and all the roots of $h_k(X)$ are in $\mathbb{F}_{p^k}$. Use the above algorithm to find an $\alpha \in \mathbb{F}_{p^k}$ such that $h_k(\alpha) = 0$. Find the minimal polynomial $g_\alpha(X)$ of α over $\mathbb{F}_p$. Then clearly $g_\alpha(X)$ will be an irreducible factor of $f(X)$.

Divide by $g_\alpha(X)$ and repeat.

Theorem 4.1. *This works.*

Proof. The only problem that may occur is that all the $h_k(X)$ are 1. Since $f(X)$ is reducible then $f = f_1^{\ell_1} \cdots f_r^{\ell_r}$. Then the roots of f_1 are in $\mathbb{F}_{p^{\deg f_1}}$ so $h_{\deg f_1} \neq 1$. $\square$

4.2 Running Time

Let α be in $\mathbb{F}_{p^k}$ and in no smaller field (easy to check using powers of Frobenius). Then the minimal polynomial has degree k so simply find a relation between $1, \alpha, \ldots, \alpha^k$ using simple linear algebra.