Factorization of polynomials in one variable over finite fields

Recall some results on finite fields.

Let G be a finite commutative group. The order of an element $a \in G$ is the smallest positive integer γ s.t. $a^\gamma = 1$.

Lemma 1 $\text{ord}(a) \mid |G| \quad \forall a \in G$ and hence $a^{|G|} = 1 \ \forall a \in G$.

Lemma 2 Let γ be the least common multiple (lcm) of the orders of the elements of G. Then $\exists$ an element of order γ. In particular $\gamma \mid |G|$.

Lemma 3 Let p, m, n be positive integers with $p \geq 2$. If $p^m - 1 \mid p^n - 1$ then $m \mid n$.

Proof: Let $n = qm + r$, with $0 \leq r \leq m-1$. Then $p^r \equiv p^n \bmod p^m - 1$ i.e. $p^r \equiv 1 \bmod p^m - 1$. Since $r < m \Rightarrow r = 0$. ∎

Proposition: $\forall a \in \mathbb{F}_q^*$, $a^{q-1} = 1$ and

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$$

Proof: $\forall a \in \mathbb{F}_q^*$, by Lemma 1 we have $a^{q-1} = 1$. Hence $a^q = a$ in $\mathbb{F}_q$. This implies that $x^q - x$ vanishes at all elements in $\mathbb{F}_q$, so $\prod_{a \in \mathbb{F}_q} (x-a) \mid x^q - x$.

Since both polynomials are monic and of same degree, They are equal.

Corollary: $\forall i = 1, \dots, p-1$ the binomial coefficient $\binom{p}{i}$ is divisible by p.

Proof: Recall that the binomial coefficient is the coefficient of x^i in $(x+1)^p$. By previous proposition we have

$$x^p - x = \prod_{a \in \mathbb{F}_p} (x-a) = \prod_{a \in \overline{\mathbb{F}_p}} (x-a+1) =$$

$$= \prod_{a \in \mathbb{F}_p} ((x+1)-a) = (x+1)^p - (x+1)$$

$$\Rightarrow (x+1)^p = x^p + 1 . \quad \blacksquare$$

Corollary: Let $f \in \mathbb{F}_q[x]$. and $A = \mathbb{F}_q[x]/(f)$ Then the Frobenius map $\phi_q : A \longrightarrow A$, $a \longmapsto a^q$ is $\mathbb{F}_q$-linear.

Proof: Let $\lambda \in \mathbb{F}_q$ and $a, b \in A$. The equality

- $\phi(\lambda a) = (\lambda a)^q = \lambda^q a^q = \lambda \phi(a)$
- $\phi(a+b) = (a+b)^q = \sum_{k=0}^{q} \binom{q}{k} a^{q-k} b^k$

$= a^q + b^q$ (by previous corollary). $\blacksquare$

Some consequences:

Proposition: $\forall c_0, \dots, c_m \in \mathbb{F}_q$, we have the following equality

$$\left(\sum_{i=0}^{m} c_i x^i \right)^q = \sum_{i=0}^{m} c_i x^{iq}$$

Proof: Immediate !

Proposition: $\forall e \geq 1$, The polynomial $x^{q^e} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ whose degree divides e.

Proof: Let $F \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n, $n \mid e$.

$n \mid e \Rightarrow \mathbb{F}_{q^e}$ contains $\mathbb{F}_{q^n}$ as subfield.

If α is a root of F in the splitting field of F over $\mathbb{F}_q$, then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$ and $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$. This means that $\alpha^{q^e} = \alpha$ and hence α is a root of $x^{q^e} - x \in \mathbb{F}_q[x]$. Thus, $F \mid x^{q^e} - x$

$\Rightarrow$ The monic irreducible polynomials occurring in the factorization of $g(x) = x^{q^e} - x$ are those whose degree divides e.

$g'(x) = -1 \in \mathbb{F}_q[x] \Rightarrow g$ has no multiple roots in the splitting field of g over $\mathbb{F}_q$. So all the factors occure exactly once. ∎

Berlekamp's Algorithm.

Assume that F is monic, separable (all roots distinct in the algebraic closure), of degree n. $F \in \mathbb{F}_q[x]$, $q = p^d$.

We look for $F_1, \dots, F_r$ s.t. $F = F_1 \cdots F_r$ and F_i are irreducible.

LINEAR ALGEBRA REDUCTION

We can consider the following map

$$\psi_F : \frac{\mathbb{F}_q[x]}{(F)} \longrightarrow \frac{\mathbb{F}_q[x]}{(F)}$$

$$G \longmapsto G^q - G$$

Since Frobenius map is linear, also this one is linear.

Studying $\ker \psi_F$ will allow to factorize F.

Proposition: A polynomial G of degree at most $n-1$ is in the kernel of $\psi_F \iff G$ is constant modulo each F_i.

Proof: $x^q - x$ factors in $\mathbb{F}_q$ and hence factors in $\mathbb{F}_q[x]/(F_i)$

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$$

Since $\mathbb{F}_q[x]/(F_i)$ is a field containing $\mathbb{F}_q$, an element $b \in \mathbb{F}_q[x]/(F_i)$ is a root of $x^q - x \Leftrightarrow$ it is a root of one of the factors of $x - a$. Hence b is a root of $x^q - x \Leftrightarrow b \in \mathbb{F}_q$.

($G^q \equiv G \bmod F \Leftrightarrow G^q \equiv G \bmod F_i \quad \forall 1 \le i \le r$
$\Leftrightarrow G^q = G$ in $\mathbb{F}_q[x]/(F_i) \Leftrightarrow G \bmod F_i \in \mathbb{F}_q$.) ∎

Denote $\hat{F}_i = F / F_i$ and observe that

$$B_i = \left(\frac{\hat{F}_i \; F_i^{-1}}{F^{-1}} \right) \bmod F$$

for $i = 1, \ldots, r$, satisfy

$$B_i \bmod F_j = \begin{cases} 1 & j = i \\ 0 & \text{otherwise} \end{cases}$$

$\Rightarrow B_i$ form a basis of $\ker \psi_F$. (Kernel is a subspace)

Hence if $G \in \ker \psi_F$, then $G = \sum_{i=1}^{r} b_i B_i$

Computing the dimension of the kernel of ψ_F, we will know how many factors F has.

Proposition: If G is a non constant polynomial in $\ker \psi_F$, then $G \bmod F_i$ are not identical constants.

Proof: Since all the F_i are distinct and irreducible by the CRT we have

$$\frac{\mathbb{F}_q[x]}{(F)} \cong \frac{\mathbb{F}_q[x]}{(F_1)} \times \cdots \times \frac{\mathbb{F}_q[x]}{(F_r)}$$

and the isomorphism is given by

$$G \bmod F \longmapsto (G \bmod F_1, \ldots, G \bmod F_r)$$

Moreover each of $\frac{\mathbb{F}_q[x]}{(F_i)}$ is a field.

Hence $\psi_F : \frac{\mathbb{F}_q[x]}{(F)} \to \frac{\mathbb{F}_q[x]}{(F)}$ can be seen as a map

$$\psi_F : \left(\frac{\mathbb{F}_q[x]}{F_1} \times \cdots \times \frac{\mathbb{F}_q[x]}{F_r}\right) \to \left(\frac{\mathbb{F}_q[x]}{F_1} \times \cdots \times \frac{\mathbb{F}_q[x]}{F_r}\right)$$

$$(G_1, \ldots, G_r) \longmapsto (\underset{\bmod F_1}{G_1^q - G_1}, \ldots, \underset{\bmod F_r}{G_r^q - G_r})$$

If all G_i are the same mod F_i, then $G = G_i \ \forall i$ because the deg of G is smaller than the deg of F.
$\Rightarrow G$ is constant, which contradicts the assumption. ∎

The key for Berlekamp algorithm is the following result.

Proposition: Let G be non constant in $\ker \psi_F$. Then $\exists\, a \in \mathbb{F}_q$ s.t. $\gcd(F, G-a) \mid F$ (non trivial division).

Proof: For $a \in \mathbb{F}_q$ we have

$$\gcd(F, G-a) = \prod F_i$$

where the product is taken on the F_i that divide $G-a$, i.e. such that $G \equiv a \bmod F_i$. Since there are at least

RT

two of such values (by previous proposition), construct, each of these gives divisors of F.

Algorithm:

Input: F separable, $\deg F = n$, $F \in \mathbb{F}_q[x]$

Output: A non trivial factor of F if F is not irreducible.

1. Computes the matrix $Q \in \mathbb{F}_q^{n \times n}$ representing ψ_F with basis $x^{n-1} \bmod f$, $x^{n-2} \bmod f$, ---, $1 \bmod f$
2. If $\operatorname{rk}(Q - I) = n-1 \Rightarrow F$ irreducible
3. Choose $G \in \operatorname{Ker} \psi_F$, non constant, $\deg(G) \leq n-1$
4. Compute $\gcd(F, G-a)$ $\forall a \in \mathbb{F}_q$ until a non trivial factor is found.

Theorem: The algorithm computes a non trivial factor of F in $O(n^\omega + (q+n) M(n) \log n)$ operations in $\mathbb{F}_q$

Proof: The first step is computing Q, in the basis $x^{n-1}, \dots, 1$.
We begin by computing $x^q \bmod F$, which costs $O(\log q)$ operations mod F and so $O(M(n) \log q)$ operations in $\mathbb{F}_q$. Then we need to compute $(x^2)^p = (x^p)^2$, $(x^3)^p = (x^p)^3$, ---, These are n multiplications mod F hence $O(nM(n))$ in total
The linear algebra part costs $O(n^\omega)$. Once a polynomial in the kernel is obtained, each gcd trial costs $O(M(n) \log n)$ operations and at most q trial are needed.

Alternative

1. Compute $x^q \bmod f$ *
2. for $i = 0, \dots, n-1$ compute $x^{qi} \bmod F = \sum_{0 \le j < n} q_{ij} x^j$

   $Q = (q_{ij})$
3. Use Gaussian elimination on $Q - Id \in \mathbb{F}_q^{n \times n}$ to compute $\dim \ker \varphi_F$ and a basis $b_1 \bmod F, \dots, b_k \bmod F$ of $\ker \varphi_F$

   If $k = 1$ return f
4. choose independent uniformly at random $c_1, \dots, c_k \in \mathbb{F}_q$

   $G = c_1 b_1 + \dots + c_k b_k$
5. $g_\ell = \gcd(G_a, F)$ until g_ℓ nontrivial.

---

* Repeated squaring (Square and multiply)

Input: $a \in R$, R ring with 1, $n \in \mathbb{N}$

Output: $a^n \in R$

1. Write $n = 2^k + m_{k-1} 2^{k-1} + \dots + m_1 2 + m_0$ $m_i \in \{0, 1\}$

   $b_k = a$
2. for $i = k-1, k-2, \dots, 0$ do

   if $m_i = 1$ then

   $b_i = b_{i+1}^2 a$

   else $b_i = b_{i+1}^2$

   end if

   end for

return b_0.

Example: $13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1$

$a^{13} = (((a^2 \cdot a))^2)^2 \cdot a$ → 3 squaring and 3 multiplications

If $R = \mathbb{F}_{17}$, $a = 8$ then

$8^{13} \bmod 17 = (((8^2 \cdot 8))^2)^2 \cdot 8 \equiv ((-4 \cdot 8))^2)^2 \cdot 8 \equiv$

$\equiv (2^2)^2 \cdot 8 \equiv 4^2 \cdot 8 \equiv -1 \cdot 8 \equiv -8 \bmod 17$

Example of Berlekamp

$f(x) = x^4 + x^2 + x + 1 \in \mathbb{F}_2[x]$

We want to factorize f using Berlekamp algorithm.

We have to compute Q.

f has degree 4, so we need to evaluate ψ_F on the monomials $\{1, x, x^2, x^3\}$.

$\psi_F(1) = 1 - 1 = 0 \longrightarrow [0, 0, 0, 0]$

$\psi_F(x) = x^2 - x = x^2 - x \bmod f \quad [0, 1, 1, 0]$

$\psi_F(x^2) = x^4 - x^2 \longrightarrow x^3 + x + 1 \bmod f \quad [1, 1, 0, 1]$

$\psi_F(x^3) = x^6 - x^3 \longrightarrow x^3 + x \bmod f \quad [1, 0, 0, 1]$

$$Q = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Find $\ker Q = \{ v : Qv = 0 \}$

$$Q \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} = 0 \iff$$

$$\begin{cases} v_2 + v_3 = 0 \\ v_1 + v_2 + v_4 = 0 \\ v_1 + v_4 = 0. \end{cases} \iff \begin{cases} v_2 = v_3 \\ v_4 = v_1 + v_2 \\ v_1 = v_4 \end{cases}$$

$v_2 = v_3 = 0$

$v_2 = 0$

$v_1 + v_4 = 0$

$$\begin{cases} v_3 = v_2 = 0 \\ v_1 + v_4 = 0 \Rightarrow v_1 = v_4 \end{cases}$$

$(1,0,0,1) \longrightarrow x^3 + 1$

For $G(x) = x^3 + 1$ compute $\gcd(F(x), x^3 + 1)$ • $a = 0$

Example of repeated squaring: Compute 3^5

$5 = (1,0,1)$ $t = 3$ $g = 3$

- $R = 1$

  $i = 2$

  $R = R \cdot g = 3$

- $i = 1$

  $e_1 = 0$

  $R = R^2 = 9$

- $i = 0$
- $e_0 = 1$

  $R = 9^2 \cdot 3 = 243$