Chapter 2

Factoring Polynomials using Drinfeld Modules

2.1 Introduction

In this chapter we construct an algorithm to factor polynomials in $\mathbb{F}_q[X]$ using Drinfeld modules. The main idea of the algorithm is similar to the idea behind H.W. Lenstra's elliptic curve method (ECM) to factor some integer $n \in \mathbb{N}$; cf. [38]. We analyse the complexity of the algorithm that we propose, and we compare the algorithm to the well-known Cantor-Zassenhaus algorithm. This chapter is accepted for publication in *Mathematics of Computation*.

Let q be a power of some prime p. Throughout this chapter we will denote $A = \mathbb{F}_q[X]$. Let $N \in A$ be a polynomial. As is well-known, it is easy to factor N as $N = \prod_i N_i$ where each N_i is a product of irreducible polynomials of degree i. Therefore, we will assume that $N = \prod_{i=1}^{k} P_i$ where each P_i is an irreducible polynomial with $\deg(P_i) = d > 1$ for all i. Moreover, we will assume that the polynomials P_i are distinct.
The basic idea behind the algorithm that we propose in this chapter is the following. A Drinfeld module φ defined over the ring A/NA equips A/NA with an A-module structure which is distinct from the natural A-module structure of A/NA. For any $b \in A/NA$ we write $\varphi_a(b)$ for the multiplication of $a \in A$ with b using the A-module structure defined by φ.
As A/NA is finite, there exists a polynomial $N' \in A$ with minimal degree such that $\varphi_{N'}(b) = 0$ for every $b \in A/NA$. If not all irreducible factors of N' have the same degree, then we can find a proper factorization of N' into polynomials N'_i such that the irreducible factors of N'_i have degree i. For any i for which $N'_i \neq 1$, the element $\varphi_{N'_i}(1)$ gives rise to a zero-divisor in A/NA and thus to a factor of N.

2.2 Drinfeld modules

Let B be an A-algebra coming from an $\mathbb{F}_q$-linear ring homomorphism $\gamma : A \longrightarrow B$. We first introduce Drinfeld modules over B.

(1) Let $B\{\tau\}$ be the free B-module generated by the elements τ^n. So its elements are

finite sums $\sum_i b_i\tau^i$ with $b_i \in B$. We can consider $B\{\tau\}$ as a *skew-polynomial ring* by equipping it with the multiplication which is given by the multiplication in B and the rule

$$b\tau^i.c\tau^j = bc^{q^i}\tau^{i+j}.$$

(2) Every element $\sum_i c_i\tau^i \in B\{\tau\}$ induces an $\mathbb{F}_q$-linear endomorphism $B \longrightarrow B$ given by $b \mapsto \sum_i c_i\tau^i(b) = \sum_i c_i b^{q^i}$. This gives a ring homomorphism

$$B\{\tau\} \longrightarrow \mathrm{End}_{\mathbb{F}_q}(B).$$

(3) We define a homomorphism on $B\{\tau\}$ as follows.

$$\partial_0 : B\{\tau\} \longrightarrow B \quad \text{by } \sum b_n\tau^n \mapsto b_0.$$

(4) Let $\varphi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,B}) = B\{\tau\}$ be a ring homomorphism; φ is called a *Drinfeld-module* if

(*i*) $\partial_0 \circ \varphi = \gamma$;

(*ii*) there is an element $a \in A$ with $\varphi(a) \neq \gamma(a)$.

So φ is $\mathbb{F}_q$-linear.

Following the usual convention, we will write φ_a instead of $\varphi(a)$ for $a \in A$. The ring homomorphism φ is determined by $\varphi_X = \sum_{i=0}^{r} b_i\tau^i$. By property (4)(*i*) we have $b_0 = \gamma(X)$.
If b_r is not nilpotent in B, then we call $r \geq 0$ the *rank* of φ. Without loss of generality we may assume that b_r is not nilpotent; cf. [41].

Remark 2.2.1. Note that this is not the usual definition of the rank of a Drinfeld module. Usually the rank is defined as a locally constant function on B, i.e., the rank is constant on each connected component of B. Our definition of rank is equals the maximum of the usual ranks on the connected components of B.

Canonically, B is an A-module via γ. Using (2) and (4), it follows that φ induces another A-module structure on B.

2.2.1 Drinfeld modules acting on A/NA

From now on, we let $B = A/NA$. In this section we describe the linear operators on B induced by $B\{\tau\}$ and, in particular, by a Drinfeld module φ. Let

$$B_j := A/P_jA.$$

Hence $B \simeq \oplus_{j=1}^{k} B_j$. Let

$$\gamma : A \longrightarrow B \quad \text{givenby} \quad X \mapsto X \bmod N.$$

Let $\varphi : A \longrightarrow B\{\tau\}$ be a Drinfeld module of rank r, and denote $\varphi_X = \sum_{i=0}^{r} b_i\tau^i$. By definition $b_0 = X \bmod N$. Moreover, we will assume that $b_r \in B^*$. Note that if $b_r \notin B^*$ and $b_r \neq 0$, then we have found a proper divisor of N, namely $\gcd(N, b_r)$.

Clearly, the map τ leaves each B_j invariant. We note three consequences of this.

(1) φ induces an A-module structure on each B_j, hence there is an isomorphism of A-modules $B \simeq \oplus_{j=1}^{k} B_j$, where the A-module structure is given by φ.

(2) τ^d is the identity on B. Namely, $B_j \simeq \mathbb{F}_{q^d}$, so τ^d is the identity on each B_j, hence also on B.

(3) τ keeps each B_j invariant, hence the operators induced by $\omega \in B\{\tau\}$ keep each B_j invariant.

Lemma 2.2.2. *The map $B\{\tau\} \longrightarrow \mathrm{End}_{\mathbb{F}_q}(B)$ has as kernel the two-sided ideal $(\tau^d - 1)$ and its image is isomorphic to*

$$\prod_j \mathrm{End}_{\mathbb{F}_q}(B_j) \simeq B\{\tau\}/(\tau^d - 1).$$

Furthermore, $\mathrm{End}_{\mathbb{F}_q}(B_j) \simeq M_d(\mathbb{F}_q)$, where $M_d(\mathbb{F}_q)$ denotes the ring of $d \times d$ matrices with coefficients in $\mathbb{F}_q$.

Proof. Because $B_j \simeq \mathbb{F}_{q^d}$, we have by general Galois theory that

$$\mathrm{End}_{\mathbb{F}_q}(B_j) = \oplus_{\rho \in \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)} B_j \rho = \oplus_{i=0}^{d-1} B_j \sigma^i$$

where σ generates $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$. This shows that the map

$$B_j\{\tau\} \longrightarrow \mathrm{End}_{\mathbb{F}_q}(B_j)$$

given by $\tau \mapsto \sigma$ is surjective. By dimension considerations we see that

$$B_j\{\tau\}/(\tau^d - 1) \simeq \mathrm{End}_{\mathbb{F}_q}(B_j).$$

As rings

$$B\{\tau\}/(\tau^d - 1) \simeq \prod_{j=1}^{k} B_j\{\tau\}/(\tau^d - 1).$$

□

Proposition 2.2.3. *Every element in $B\{\tau\}/(\tau^d - 1)$ can be represented by $\varphi_X \in B\{\tau\}$ where φ is a Drinfeld module of rank at most $d + 1$.*

Proof. Any element in $B\{\tau\}/(\tau^d - 1)$ can be represented by some $\omega = \sum_{i=0}^{d-1} a_i \tau^i \in B\{\tau\}$. Put

$$b_0 = X \bmod N, b_d = a_0 - b_0, \text{ and } b_i = a_i$$

for $i = 2, \ldots, d-1$. If $b_d = 0$, then we put $b_1 = a_1$ and $b_{d+1} = 0$. Otherwise we put $b_1 = a_1 - 1$ and $b_{d+1} = 1$. Let φ be the Drinfeld module given by $\varphi_X = \sum_{i=0}^{d+1} b_i \tau^i$, then φ is a Drinfeld module of rank at most $d + 1$, and φ_X represents by construction the same element in $\mathrm{End}_{\mathbb{F}_q}(B)$ as ω. □

2.3 The algorithm

In this section we describe the algorithm and illustrate it with an example. Let φ be a Drinfeld module of rank at most $d+1$, then φ_X defines an $\mathbb{F}_q$-linear operator on B. Let $f \in A$ be the characteristic polynomial of this linear operator. Consequently,

$$\varphi_f = f(\varphi_X) \equiv 0 \bmod (\tau^d - 1).$$

By Lemma 2.2.2 it follows that φ_X also induces an $\mathbb{F}_q$-linear operator on each B_j, hence gives rise to characteristic polynomials $f_j \in A$, with $f = \prod_{j=1}^{k} f_j$.
In this way we associate to each polynomial P_i a polynomial f_i of the same degree d, but f_i may very well be reducible. Let g_d be the product of all f_i's which are irreducible, and let g_r be the product of the other f_i's. Then we have $f = g_d g_r$. These elements g_d and g_r can easily be computed. If the factorization $f = g_d g_r$ is not trivial, then it gives rise to a proper divisor of N:

Proposition 2.3.1. *If $1 \neq g_d \neq f$, then for all $b \in B^*$ the element $\gcd(\varphi_{g_d}(b), N)$ is a proper divisor of N.*

Proof. Because $g_d \neq 1$ there is an i such that $\varphi_{g_d}(b) = 0 \bmod P_i$. In fact this is exactly the case for all i with $f_i \mid g_d$. If f_i does not divide g_d, then let $a \in A$ be the polynomial of minimal degree such that $\varphi_a(b) = 0 \bmod P_i$, then $a \mid f_i$, hence $\gcd(a, g_d) = 1$ and thus $\varphi_{g_d}(b) \neq 0 \bmod P_i$. This shows that $\varphi_{g_d}(b)$ is a zero divisor. □

If $d = 1$, then the f_i are all of degree 1, so for all choices of φ we have $g_d = f$. So our algorithm will not give anything interesting in this case. One can also see this in a different way. If $d = 1$, then τ acts as the identity, hence φ_h acts as multiplication with $\gamma(h) = h \bmod N$ for all $h \in A$, i.e., φ induces the same A-module structure on B as γ.
The next case is $d = 2$. We will illustrate the suggested algorithm in an example for this case.

Example 2.3.2. Suppose $d = 2, p > 2$. We choose $\varphi_X = X + c\tau$ with $c \in \mathbb{F}_q^*$. We take $N = \prod_{i=1}^{k} P_i$ such that $P_i = X^2 + a_i X + b_i \in \mathbb{F}_q[X]$. Then on $B_i = A/P_i A$ we have

$$\varphi_X(1) = X + c, \quad \varphi_X(X) = X^2 + cX^q = -a_i X - b_i - c(X + a_i).$$

Hence on the basis $\{1, X\}$ of B_i the matrix of φ_X is given by

$$\begin{pmatrix} c & -ca_i - b_i \\ 1 & -a_i - c \end{pmatrix}.$$

The characteristic polynomial of φ_X on B_i is $f_i = \lambda^2 + a_i\lambda + b_i - c^2$. If we fix P_i, for how many c's is $f_i = P_i - c^2$ still irreducible? The discriminant of f_i is

$$a_i^2 - 4(b_i - c^2) = D + 4c^2.$$

Here D is the discriminant of P_i. Hence f_i is reducible iff $D + 4c^2$ is a square in $\mathbb{F}_q$. Now applying Theorem 5.48 in [39] to the polynomial $g(X) = 4X^2 + D$ and noting that

$g(0) = D \notin (\mathbb{F}_q^*)^2$ gives that the fraction of c's in $\mathbb{F}_q^*$ such that $D + 4c^2$ is a square in $\mathbb{F}_q$ equals

$$\begin{cases} \frac{1}{2} \cdot \frac{q+1}{q-1} & \text{if } -1 \text{ is not a square in } \mathbb{F}_q; \\ \frac{1}{2} & \text{if } -1 \text{ is a square in } \mathbb{F}_q. \end{cases}$$

This shows that for relatively large q one may expect that f_i is irreducible with a probability of $\frac{1}{2}$. Hence the probability that applying this computation once gives rise to a decomposition of N is approximately $1 - \frac{1}{2}^k - \frac{1}{2}^k \geq \frac{1}{2}$, because $k \geq 2$. There is one drawback, which is due to the fact that we chose φ_X in such a special way. E.g., when $N = P_1P_2$ and $a_1^2 - 4b_1 = a_2^2 - 4b_2$, then there is no c for which the described algorithm will give a decomposition. In a general setting, i.e., where $\varphi_X = c_0X + c_1\tau, c_i \in B$, this problem disappears as we will see in Section 2.4.

The algorithm which appears from the previous considerations is the following:

Algorithm 2.3.3.

Let $N \in A$ be a product of monic irreducible polynomials P_i which have all degree $d > 1$.

(1) Choose some Drinfeld-module, given by φ_X. We regard φ_X as a linear operator. Therefore, it is given by a d-tuple $a = (a_0, \ldots, a_{d-1})$ with $a_i \in B$. Represent φ_X as a matrix by computing $\varphi_X(1), \ldots, \varphi_X(X^{n-1})$.

(2) Compute the characteristic polynomial f of φ_X.

(3) Compute g_d, the product of all the irreducible polynomials of degree d in f, by: For $l = 1$ upto $d - 1$, $f \leftarrow f/\gcd(X^{q^l} - X, f)$.

(4) Finally, compute $\gcd(g_d(\varphi_X)(1), N)$.

(5) This either gives a factor of N or one starts again with step 1.

Remark 2.3.4. Note that in step 1. one should not choose the Drinfeld module φ of the form $\varphi_X = X + \sum_{i<\infty} b_i\tau^{di} \in B\{\tau\}$, because this Drinfeld module induces the same A-action on B as γ does. These Drinfeld modules correspond exactly to d-tuples $(a_0, 0, \ldots, 0)$. The other d-tuples correspond to Drinfeld modules which give an A-action on B different from the one induced by γ.
By Lemma 2.2.2 we see that there exists an $M \in \mathrm{End}_{\mathbb{F}_q} B$ such that we have for its characteristic polynomial $f = g_dg_r$ with g_d and g_r are both non-constant. In this algorithm we consider all Drinfeld modules upto rank $d + 1$, hence by Proposition 2.2.3 and Proposition 2.3.1 it will factor N.
Note that there seems no reason to consider only Drinfeld modules up to a rank smaller than $d + 1$. E.g., the final remark of Example 2.3.2 shows that considering only rank 1 Drinfeld modules when $d = 2$ is not enough to factor N.

Remark 2.3.5. In this chapter we consider Algorithm 2.3.3, without looking at fancy ways of implementing it. One may expect that the complexity of the algorithm will improve if one takes implementation details into account and changes the algorithm accordingly. In the following section, we will compute the complexity of the algorithm, assuming that in steps 1. up to 5. classical methods are being used.

2.4 Complexity analysis

In this section we give a complexity analysis of the algorithm described in 2.3.3. In the first part we compute with which probability the algorithm decomposes N in one step; cf. Proposition 2.4.3. The second part computes the number of multiplications needed in one step; cf. Proposition 2.4.4.

Lemma 2.4.1. *The number of matrices in $M_d(\mathbb{F}_q)$ with a given characteristic polynomial $g \in \mathbb{F}_q[X]$ which is irreducible, monic and of degree d is $\prod_{i=1}^{d-1}(q^d - q^i)$.*

Proof. This is a special case of Theorem 2 in [47]. □

Proposition 2.4.2. *Let $d > 1$. Let $\delta = \frac{1}{q-1}$ and denote with α the fraction of operators in $M_d(\mathbb{F}_q)$ which have an irreducible characteristic polynomial. Then for $q \geq 5$*

$$\frac{1}{d} > \alpha > \frac{1}{d}(1-\delta)(1-2\delta).$$

If $q \gg d$, then α is approximately $\frac{1}{d}$.

Proof. Let $x_d = \#\{\text{monic irreducible polynomials of degree } d \text{ in } \mathbb{F}_q[X]\}$. According to Lemma 2.4.1 there are $(q^d - q)\cdots(q^d - q^{d-1})$ matrices with the same irreducible characteristic polynomial of degree d, hence a fraction $\alpha = \frac{x_d(q^d-q)\cdots(q^d-q^{d-1})}{q^{d^2}} = \frac{1}{q^d}x_d\beta$ with $\beta = (1-q^{1-d})\cdots(1-q^{-1}) < 1$ of all matrices has an irreducible characteristic polynomial.
The well-known estimate $\frac{1}{d}q^d > x_d > \frac{1}{d}q^d(1 - \frac{q}{q-1}q^{\frac{-1}{2}d}) \geq (1-\delta)$, where the latter is true when $d \geq 2$, implies that $\frac{1}{d} > \alpha > \frac{1}{d}\beta(1-\delta)$.
Now we estimate β. If $|x| < 1$, then $|\log(1+x)| \leq \frac{1}{1-|x|}|x|$. Because $1 + \delta = \frac{1}{1-\frac{1}{q}}$, this estimate implies $|\log(1-q^{-i})| \leq (1+\delta)q^{-i}$ for $i = 1, \ldots, d-1$ and thus $|\log(\beta)| \leq (1+\delta)\frac{q^{-1}-q^{-d}}{1-q^{-1}} \leq (1+\delta)\delta$.
Also $|e^x - 1| \leq \frac{|x|}{1-|x|}$, hence $|\beta - 1| \leq \frac{(1+\delta)\delta}{1-(1+\delta)\delta} \leq 2\delta$, where the latter inequality is true when $\delta \leq \frac{1}{4}$, i.e., $q \geq 5$. □

Proposition 2.4.3. *Let α be as in Proposition 2.4.2. Then we may expect that after $\frac{1}{1-\alpha^k-(1-\alpha)^k}$ choices of a Drinfeld module, Algorithm 2.3.3 gives a decomposition of N. If $q \gg d$, this number is approximately $\frac{d^k}{d^k-(d-1)^k-1}$.*

Proof. The algorithm gives according to Proposition 2.3.1 a decomposition when g_d, the part of the characteristic polynomial $f = \prod_i f_i$ of φ_X which consists of all f_i's which are irreducible, is neither f nor 1. According to Proposition 2.4.2, $g_d = f$ with probability α^k, and $g_d = 1$ with probability $(1-\alpha)^k$. If $q \gg d$, then α is approximately $\frac{1}{d}$. □

Proposition 2.4.4. *One step of Algorithm 2.3.3 takes $n^2\log(q) + dn^3$ multiplications in $\mathbb{F}_q$ asymptotically. If $q \gg n$, then this is asymptotically $n^2\log(q)$.*

Proof. We count the number of multiplications in $\mathbb{F}_q$ in each step of Algorithm 2.3.3; $q \gg d$, hence α is approximately $\frac{1}{d}$.

(1) To compute the matrix of φ_X one needs to compute $\varphi_X(X^i)$ mod N for $i = 0, \ldots, n-1$, where $\varphi_X = \sum_{i=0}^{d-1} a_i \tau^i$. First we compute X^{iq^j} in the following standard way. Computing X^q takes $\log(q)$ multiplications in B. So computing the vector $(X^{iq})_{i=0}^{n-1}$ takes $\log(q)+n-2$ multiplications in B. If we write $X^q = \sum_{i=0}^{n-1} b_i X^i$ with $b_i \in \mathbb{F}_q$, then $X^{q^2} = \sum_{i=0}^{n-1} b_i X^{iq}$. Hence computing X^{q^2} will cost n^2 multiplications in $\mathbb{F}_q$. Thus computing the elements $X^q, \ldots, X^{q^{d-1}}$ takes $(d-2)n^2$ multiplications in $\mathbb{F}_q$.
Finally, we compute $\varphi_X(X^j)$ by first computing the vector $(a_i X^{q^i})_{i=0}^{d-1}$. Adding the coefficients of this vector gives $\varphi_X(X)$. Computing $(a_i X^{q^i} X^{q^i}) = (a_i X^{2q^i})_{i=0}^{d-1}$ gives $\varphi_X(X^2)$ etc. This takes $(d-1)(n-1)$ multiplications in B.
One multiplication in B takes n^2 multiplications in $\mathbb{F}_q$, hence we see that this step is of order $O(n^2 \log(q) + dn^3)$ computations in $\mathbb{F}_q$.

(2) According to [7, p. 55], the *Hessenberg* algorithm there described will take order $O(n^3)$ multiplications in $\mathbb{F}_q$.

(3) This is just the first step of the Berlekamp algorithm. Computing $X^{q^l} - X$ mod f is done as in step 1., hence this will take asymptotically $n^2 \log(q) + ln^2$ multiplications in $\mathbb{F}_q$, and the gcd of 2 polynomials of degree n and $n-1$ will take asymptotically n^2 multiplications in $\mathbb{F}_q$. Hence this does not add anything asymptotically to step (1).

(4) This will take $\deg(g_d)$, which is d times the number of irreducible f_i's, matrix multiplications. Given the fact that $\alpha \approx \frac{1}{d}$, we expect that $\deg(g_d) = k$. To compute $\varphi_{X^j}(1)$ we only need to compute the first column of φ_{X^j}, which is φ_X times the first column of $\varphi_{X^{j-1}}$. So to compute $\varphi_X(1), \ldots, \varphi_{X^k}(1)$ takes kn^2 multiplications in $\mathbb{F}_q$. Hence to compute $g_d(\varphi_X(1))$ takes $kn^2 + kn$ multiplications. Hence asymptotically kn^2 in $\mathbb{F}_q$.

This sums asymptotically to $n^2 \log(q) + dn^3$. Hence if $q \gg n$, this sums asymptotically to $n^2 \log(q)$. □

Remark 2.4.5. Finally, we compare this method to the well-known Cantor-Zassenhaus algorithm. As they show in their paper [5], the propability of successfully finding a factor of N in one step of the algorithm is about $1 - 2^{1-k}$, where k is the number of irreducible factors of N. And one step of their algorithm, using classical methods, is of complexity $O(dn^2 + n^2 \log(q))$.
We see that according to Proposition 2.4.3, the probability of finding a factor in one step is for large q approximately $1 - \frac{(d-1)^k+1}{d^k}$. In case d is large compared to k, this factor is approximately $\frac{k}{d}$. In this case the proposed algorithm is much worse than Cantor-Zassenhaus.
If $k \geq d$, then $1 - \frac{(d-1)^k+1}{d^k} > \frac{1}{2}$ and in fact tends to 1 if k is much larger than d. E.g., when $d = 2$, then we see that $1 - \frac{(d-1)^k+1}{d^k} = 1 - 2^{1-k}$.
The complexity of one step of the proposed Algorithm 2.3.3 is $O(dn^3 + n^2 \log(q))$, which can compete with the complexity of Cantor-Zassenhaus if dn^3 is not of a higher order than $n^2 \log(q)$.
This means that for $q \gg n$ and $k \geq d$ Algorithm 2.3.3 may be expected to be as efficient as Cantor-Zassenhaus's algorithm.