MATHEMATICS OF COMPUTATION
Volume 73, Number 245, Pages 317–322
S 0025-5718(03)01598-9
Article electronically published on August 7, 2003

# FACTORING POLYNOMIALS OVER FINITE FIELDS WITH DRINFELD MODULES

G. J. VAN DER HEIDEN

ABSTRACT. In the following, we describe a way of factoring polynomials in $\mathbb{F}_q[X]$ with Drinfeld modules. We furthermore analyse the complexity of the algorithm and compare it to the well-known Cantor-Zassenhaus algorithm.

## 1. Defining $\mathbb{F}_q[X]$-module structures with Drinfeld modules

Throughout this paper we will denote $A = \mathbb{F}_q[X]$, where $q$ is a power of some prime $p$, and $N \in A$ for the polynomial which is to be factored. Let $B$ be an $A$-algebra coming from an $\mathbb{F}_q$-linear ring homomorphism $\gamma : A \longrightarrow B$.

(1) $B\{\tau\}$ is the *skew-polynomial ring* which consists as set of all finite expressions $\sum_{n\geq 0} b_n\tau^n, b_i \in B$, and $B\{\tau\}$ has addition and multiplication defined by

$$\sum_{n\geq 0} b_n\tau^n + \sum_{n\geq 0} c_n\tau^n = \sum_{n\geq 0}(b_n + c_n)\tau^n, \quad b_i\tau^i.c_j\tau^j = b_i c_j^{q^i}\tau^{i+j},$$

where $b_n + c_n$ is addition and $b_i c_j^{q^i}$ is multiplication in $B$.

(2) We define a homomorphism on $B\{\tau\}$ as follows:

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

(3) Let $\varphi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,B}) = B\{\tau\}$ be a ring homomorphism; $\varphi$ is called a *Drinfeld module* if $\partial_0 \circ \varphi = \gamma$. This property implies that a Drinfeld module $\varphi$ is $\mathbb{F}_q$-linear and hence is completely given by the image of $X \in A$.

In the following we will write $\varphi_a$ instead of $\varphi(a)$ for $a \in A$. If we denote $\varphi_X = \sum_{i=0}^{r} b_i\tau^i$, then $b_0 = \gamma(X)$. If moreover $b_r$ is not nilpotent in $B$, then we call $r \geq 0$ the rank of $\varphi$. In fact, without loss of generality we may assume that $b_r$ is not nilpotent; cf. [Mat97].

Canonically $B$ is an $A$-module via $\gamma$. Every $\sum_i c_i\tau^i \in B\{\tau\}$ induces an $\mathbb{F}_q$-linear endomorphism $B \longrightarrow B$ by $\sum_i c_i\tau^i(b) = \sum_i c_i b^{q^i}$. This gives us a ring homomorphism

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

In particular this means that for all $a \in A$, $\varphi_a$ induces such a map. One checks easily that $\varphi$ gives rise in this way to a new $A$-module structure on $B$ via $(a, b) \mapsto \varphi_a(b)$.

Received by the editor July 13, 2001 and, in revised form, January 25, 2002.
2000 *Mathematics Subject Classification.* Primary 11G09, 13P05.
The author was supported by NWO Grant 613.007.040.

## 2. Drinfeld modules acting on $A/NA$

From now on assume $B = A/NA$. In this section we describe the linear operators on $B$ induced by $B\{\tau\}$ and in particular by a Drinfeld module $\varphi$. We will assume that $N = \prod_{i=1}^{k} P_i$, where the $P_i$ are distinct monic, irreducible polynomials of the same degree $d$. We write $n = \deg(N)$. This notation will be used throughout the rest of this paper. This form of $N$ can easily be achieved by the first step of Berlekamp's algorithm: replace $N$ by $\gcd(N, X^{q^d} - X)$ and subsequently divide out $\gcd(N, X^{q^l} - X)$ for all $l \mid d, l \neq d$.

We write $B_j = A/P_j A$, hence $B \simeq \bigoplus_{j=1}^{k} B_j$. Let $\gamma : A \longrightarrow B$ be the natural map given by $X \mapsto X \mod N$. Let $\varphi : A \longrightarrow B\{\tau\}$ be a Drinfeld module of rank $r$ and $\varphi_X = \sum_{i=0}^{r} b_i \tau^i$. By choice of $\gamma$, $b_0 = X \mod N$. Moreover we assume that $b_r \in B^*$. This is not a restrictive assumption, because for our application $b_r \notin B^*$ means that we have found a proper divisor of $N$, namely $\gcd(N, b_r)$, which is exactly the goal of the algorithm we want to find.

Because the natural map $B \longrightarrow B_j$ given by $b \mapsto b \mod P_j$ is an $\mathbb{F}_q$-linear ring homomorphism, the $q$-Frobenius map $\tau : B \longrightarrow B$ induces a map $\tau\,|_{B_j} : B_j \longrightarrow B_j$, the $q$-Frobenius on $B_j$, such that $\tau(b) \mod P_j = \tau\,|_{B_j}\,(b \mod P_j)$. We could also say that $\tau$ leaves each $B_j$ invariant. We note three consequences of this.

(1) $\varphi$ induces an $A$-module structure on each $B_j$; hence there is an isomorphism of $A$-modules $B \simeq \bigoplus_{j=1}^{k} B_j$, where the $A$-module structure is given by $\varphi$.
(2) $\tau^d$ is the identity on $B$. Note that $B_j \simeq \mathbb{F}_{q^d}$, which implies that $\tau^d$ is the identity on each $B_j$, hence on $B$.
(3) $\tau$ keeps each $B_j$ invariant; hence the operators induced by $\omega \in B\{\tau\}$ keep each $B_j$ invariant.

**Lemma 2.1.** *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

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

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

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

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

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

which proves the lemma. □

**Proposition 2.2.** *Every element in $B\{\tau\}/(\tau^d - 1)$ can be represented by $\varphi_X \in B\{\tau\}$, where $\varphi$ is a Drinfeld module of rank at most $d+1$.*

*Proof.* Any element in $B\{\tau\}/(\tau^d - 1)$ can be represented by some $\omega = \sum_{i=0}^{d-1} a_i\tau^i \in B\{\tau\}$. We choose $b_i \in B, i = 0, \ldots, d+1$, such that $b_0 = X \mod N, b_i = a_i$ for $1 \le i \le d-1$ and $b_d = a_0 - b_0$. If $b_d$ is not nilpotent, we choose $b_{d+1} = 0$; otherwise we choose $b_{d+1} = 1$. With this choice of the $b_i$'s, $\varphi_X = \sum_{i=0}^{d+1} b_i\tau^i$ defines a Drinfeld module $\varphi$ of rank at most $d+1$, and $\varphi_X$ represents by construction the same element in $\mathrm{End}_{\mathbb{F}_q}(B)$ as $\omega$. □

## 3. The algorithm

In this section we describe the algorithm and illustrate it with an example. If $\varphi$ is some Drinfeld module of rank at most $d+1$, then $\varphi_X \equiv \sum_{i=0}^{d-1} b_i\tau^i \mod (\tau^d - 1) \in B\{\tau\}/(\tau^d - 1)$. This is an $\mathbb{F}_q$-linear operator on $B$; hence it has a characteristic polynomial, say $f \in A$, such that $f(\sum_{i=0}^{d-1} b_i\tau^i) \equiv 0 \mod (\tau^d - 1)$. In particular $\varphi_f = f(\varphi_X) \equiv 0 \mod (\tau^d - 1)$.

From Lemma 2.1 it follows that $\varphi_X$ also induces an $\mathbb{F}_q$-linear operator on each $B_j$; hence it gives rise to polynomials $f_j \in A$, such that $f = \prod_{j=1}^{k} f_j$.

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. We decompose $f$ as $f = g_d g_r$, where $g_d$ is a product of all $f_i$'s which are irreducible and $g_r$ consists of the other $f_i$'s.

**Proposition 3.1.** *If $1 \ne g_d \ne f$, then for all $b \in B^*$, $\gcd(\varphi_{g_d}(b), N)$ is a proper divisor of $N$.*

*Proof.* Because $g_d \ne 1$ there is an $i$ such that $\varphi_{g_d}(b) = 0 \mod P_i$. 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 $\varphi_a(b) = 0 \mod P_i$. Then $a \mid f_i$. Hence $\gcd(a, g_d) = 1$ and thus $\varphi_{g_d}(b) \ne 0 \mod P_i$. 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 $\varphi$, $g_d = f$. Henceforth this case will not be interesting. One can also see this in a different way. If $d = 1$, then $\tau$ acts as the identity. Hence $\varphi_h$ acts as multiplication with $\gamma(h) = h \mod N$ for all $h \in A$; i.e., $\varphi$ induces the same $A$-module structure on $B$ as $\gamma$.

The next case is $d = 2$. We will illustrate the suggested algorithm in an example for this case.

**Example 3.2.** Suppose $d = 2, p > 2$. We choose $\varphi_X = X + c\tau, c \in \mathbb{F}_q^*$. We take $N = \prod_{i=1}^{k} P_i$, such that $P_i = X^2 + a_iX + b_i \in \mathbb{F}_q[X]$. Then on $B_i = A/P_iA$,

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

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

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

The characteristic polynomial of $\varphi_X$ 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 $a_i^2 - 4(b_i - c^2) = D + 4c^2$, where $D$ 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 [LN97] to the polynomial

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

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

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 $\varphi_X$ in such a special way. E.g., when $N = P_1 P_2$ 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 $\varphi_X = c_0 X + c_1 \tau, c_i \in B$, this problem disappears as we will see in Section 4.

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

**Algorithm 3.3.**

(1) Choose some Drinfeld module $\varphi_X$, which we regard as a linear operator; hence it is given by a $d$-tuple $a = (a_0, \ldots, a_{d-1})$, with $a_i \in B$. Represent $\varphi_X$ as a matrix by computing $\varphi_X(1), \ldots, \varphi_X(X^{n-1})$.
(2) Compute the characteristic polynomial $f$ of $\varphi_X$.
(3) Compute $g_d$, the product of all the irreducible polynomials of degree $d$ in $f$, by: For $l = 1$ up to $d-1$, $f \leftarrow f/\gcd(X^{q^l} - X, f)$.
(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* 3.4. Note that in step (1) one should not choose the Drinfeld module $\varphi$ 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 $\gamma$ 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 $\gamma$.

By Lemma 2.1 we see that there exists an $M \in \mathrm{End}_{\mathbb{F}_q} B$, such that the characteristic polynomial $f$ of $M$ splits as $f = g_d g_r$, such that both $g_d$ and $g_r$ are not constant, where we use the same notation $g_d$ and $g_r$ as above. In this algorithm we consider all Drinfeld modules up to rank $d+1$; hence by Propositions 2.2 and 3.1 it will factor $N$. Note that there is no trivial reason to consider only Drinfeld modules up to rank smaller than $d+1$. E.g., the final remark of Example 3.2 shows that considering only rank 1 Drinfeld modules when $d = 2$ is not enough to factor $N$.

*Remark* 3.5. In this paper we consider Algorithm 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.

## 4. Complexity Analysis

In this section we give a complexity analysis of the algorithm described in Algorithm 3.3. In the first part we compute with what probability the algorithm gives a decomposition of $N$ in one step; cf. Proposition 4.3. The second part computes the number of multiplications in one step; cf. Proposition 4.4.

**Lemma 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 Theorem 2 in [Rei61]. □

**Proposition 4.2.** *Let $\delta = \frac{1}{q-1}$ and denote by $\alpha$ the proportion of operators in $M_d(\mathbb{F}_q)$ which have an irreducible characteristic polynomial. Then for $q > 5$*

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

*If $q \gg d$, then $\alpha$ 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 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 proportion $\alpha = \frac{x_d(q^d-q)\cdots(q^d-q^{d-1})}{q^{d^2}} = \frac{1}{q^d}x_d\beta$, with $\beta = (1-q^{1-d})\cdots(1-q^{-1}) < 1$ of all matrices has 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 $\beta$. 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 $|e^x - 1| \leq \frac{|x|}{1-|x|}$, and 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 4.3.** *Let $\alpha$ be as in Proposition 4.2. Then we may expect that after $\frac{1}{1-\alpha^k-(1-\alpha)^k}$ choices of a Drinfeld module, Algorithm 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 3.1 a decomposition when $g_d$, the part of the characteristic polynomial $f = \prod_i f_i$ of $\varphi_X$ which consists of all $f_i$'s which are irreducible, is neither $f$ nor 1. According to Proposition 4.2 $g_d = f$ with probability $\alpha^k$ and $g_d = 1$ with probability $(1-\alpha)^k$. If $q \gg d$, then $\alpha$ is approximately $\frac{1}{d}$. □

**Proposition 4.4.** *One step of Algorithm 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 3.3; $q \gg d$, and hence $\alpha$ is approximately $\frac{1}{d}$.

(1) To compute the matrix of $\varphi_X$, 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 $X^q = \sum_{i=0}^{n-1} b_iX^i$ with $b_i \in \mathbb{F}_q$, then $X^{q^2} = \sum_{i=0}^{n-1} b_iX^{iq}$; 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 computing the vector $(a_iX^{q^i})_{i=0}^{d-1}$, which gives $\varphi_X(X)$ by adding all components. Now computing $(a_iX^{q^i}X^{q^i}) = (a_iX^{2q^i})_{i=0}^{d-1}$ 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 [Coh93, 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 $\varphi_{X^j}$, which is $\varphi_X$ times the first column of $\varphi_{X^{j-1}}$. So to compute $\varphi_X(1),\dots,\varphi_{X^k}(1)$ 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* 4.5. Finally, we compare this method to the well-known Cantor-Zassenhaus algorithm. As they show in their paper [CZ81], the probability 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 components. And one step of their algorithm, using classical methods as is done in this paper, is of complexity $O(dn^2+n^2\log(q))$.

We see that according to Proposition 4.3, the probability of finding a factor in one step is for large $q$ about $1-\frac{(d-1)^k+1}{d^k}$. 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 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 3.3 may be expected to be as efficient as Cantor-Zassenhaus's algorithm.

## References

[Coh93] H. Cohen. *A course in computational algebraic number theory*. Springer-Verlag, Berlin, 1993. MR **94i:**11105

[CZ81] D.G. Cantor and H. Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Math. Comp.*, 36(154):587–592, 1981. MR **82e:**12020

[LN97] R. Lidl and H. Niederreiter. *Finite fields*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn. MR **97i:**11115

[Mat97] B. H. Matzat. Introduction to drinfeld modules. In *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, pages 3–16. World Sci. Publishing, River Edge, NJ, 1997. MR **99i:**11045

[Rei61] I. Reiner. On the number of matrices with given characteristic polynomial. *Illinois J. Math.*, 5:324–329, 1961. MR **25:**3053

Vakgroep Wiskunde RuG, P.O. Box 800, 9700 AV Groningen, The Netherlands
*E-mail address*: gertjan@math.rug.nl