Acta Math. Univ. Comenianae
Vol. LXXX, 2 (2011), pp. 213–219

ON EXPLICIT FORMULAE AND LINEAR RECURRENT SEQUENCES

R. EULER AND L. H. GALLARDO

Abstract. We notice that some recent explicit results about linear recurrent sequences over a ring R with 1 were already obtained by Agou in a 1971 paper by considering the euclidean division of polynomials over R. In this paper we study an application of these results to the case when $R = \mathbb{F}_q[t]$ and q is even, completing Agou's work. Moreover, for even q we prove that there is an infinity of indices i such that $g_i = 0$ for the linear recurrent, Fibonacci-like, sequence defined by $g_0 = 0$, $g_1 = 1$, and

$$g_{n+1} = g_n + \Delta g_{n-1}$$

for $n > 1$, where Δ is any nonzero polynomial in $R = \mathbb{F}_q[t]$. A new identity is established.

1. Introduction

Let R be a commutative ring with 1. In a nice, but little known paper of 1971, Agou [**2**] (see also [**1**]) obtained explicit expressions of the remainder and the quotient of the euclidean division of a polynomial $f \in R[x]$ by a polynomial $g \in R[x]$. On the other hand Belbachir and Bencherif [**3**], generalizing some work of McLaughlin [**7**], recently obtained explicit values of the coefficients appearing in the decomposition of the r-th power of a square matrix A of order n over R, in terms of some special R-linear combinations of the powers A^k with $0 \leq k < n$. The key of their results comes from obtaining the explicit expression of the general term of a linear recurrent sequence of order n in terms of the coefficients of the characteristic polynomial C of the sequence. It turns out (see Section 2) that the main results of the above papers are simple consequences of the main result of Agou and that indeed these results are contained in Agou's paper. Agou gives a finite field application of his results, more precisely, he proved the identity

$$(1) \qquad (a^2 + 4b)^{\frac{q-1}{2}} = \sum_{u+2v=q-1, u\geq 0, v\geq 0} \binom{u+v}{u} a^u b^v.$$

that holds for elements a, b of the finite field $\mathbb{F}_q$ of cardinal q, by considering the special case of a division by a polynomial of degree 2 over $\mathbb{F}_q[t]$. Observe that

Received June 10, 2010.
2010 *Mathematics Subject Classification.* Primary 11T55, 11T06, 11B39.
Key words and phrases. Polynomials; euclidean division; finite fields; even characteristic.

when q is even, the identity is trivial. The object of this paper is to study the case q even, in the more general setting of the ring $R = \mathbb{F}_q[t]$. Our main results are:

a) We establish the identity (2) over the ring $R = \mathbb{F}_q[t]$, q even as an analogue of the identity (1).

   Applying the identity (2) to the numerator and denominator of B_Q we can easily deduce (no details given) an identity of the form $B_Q^{q-1} = \frac{f(d)}{f(c^2)}$, where f is a polynomial for the Berlekamp discriminant $B_Q = \frac{d}{c^2}$ of the quadratic polynomial $Q = x^2 + cx + d$.

b) A Fibonacci-like sequence defined over the ring of polynomials $R = \mathbb{F}_q[t]$, where q is a power of 2, takes the value 0 infinitely many times.

More precisely we prove the following theorems.

Theorem 1. *Let q be a power of 2. Let $b \in \mathbb{F}_q[t]$ be a nonzero polynomial. Put $a = b + 1$. The following identity holds in the ring $R = \mathbb{F}_q[t]$*

$$b^{q-2} = C + D, \tag{2}$$

$$C = \sum_{u+2v=q-2, u\geq 0, v\geq 0} \binom{u+v}{u} a^u b^v.$$

and

$$D = \sum_{u+2v=q-3, u\geq 0, v\geq 0} \binom{u+v}{u} a^u b^v.$$

Theorem 2. *Let q be power of 2. Given any nonzero polynomial $\Delta \in R = \mathbb{F}_q[t]$, the sequence of polynomials of R defined by $g_0 = 0, g_1 = 1$,*

$$g_{n+1} = g_n + \Delta g_{n-1},$$

satisfies $g_i = 0$ for an infinity of indices i.

Observe that in Theorem 2 we consider the most difficult case that arises (since the degree of the characteristic polynomial of the sequence equals the characteristic of the coefficient ring) among all possible Fibonacci-like sequences defined over $\mathbb{F}_q[t]$ where q is any power of a prime number p (odd or even).

Let q be any power of 2. The reason why in Theorem 2 we consider the special degree 2 polynomial $S = x^2 + x + \Delta \in \mathbb{F}_q[t][x]$ (as the characteristic polynomial of the sequence (g_i)) instead of the more general one $G = Cx^2 + Ax + B \in \mathbb{F}_q[t][x]$ is that Cherly et al. [**4**] proved that the study of the roots of the latter may be reduced to the study of the roots of the former. Moreover, Gallardo et al. [**5**] constructed an algorithm to determine the roots of G in $\mathbb{F}_q[t]$ without factoring G.

2. Agou's main result

Agou [**1**] proved the following result.

Lemma 1. *Let R be a ring with 1. Let $S = x^n - s_1x^{n-1} - \cdots - s_n \in R[x]$ be a polynomial of degree $n > 0$. Let $k > 0$ be a positive integer. Let $T = \sum_{j=0}^{n-1} t_{k,j}x^j$ be the remainder of the euclidean division (long division) of the monomial $M = x^{k+n-1}$ by the polynomial S in $R[x]$. Then for $j = 0, \ldots, n-1$, one has*

$$t_{k,j} = \sum_{\substack{u_1+2u_2+\cdots+nu_n=k+n-j-1,\\ u_i\geq 0, i=1,\ldots,n}} \left(\frac{(u_1 + \cdots + u_n - 1)!}{u_1! \cdots u_n!} \sum_{t=0}^{j} u_{n-t} \right) s_1^{u_1} \cdots s_n^{u_n}.$$

3. Consequences of Agou's result

Throughout this section the coefficients of polynomials and the matrix entries are elements of a fixed commutative ring R with 1.

J. McLaughlin [**7**] proved it as his main result (which also appeared as [**3**, Theorem 1])

Proposition 1. *The n-th power of a 2×2 matrix $M = (m_{i,j})$ of trace t and determinant d is given by*

$$M^n = \begin{bmatrix} y_n - m_{2,2}y_{n-1} & m_{1,2}y_{n-1} \\ m_{2,1}y_{n-1} & y_n - m_{1,1}y_{n-1} \end{bmatrix}$$

$$y_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k} t^{n-2k}(-d)^k.$$

Proof. This follows as a special case of a power of a 2×2 matrix from the formula of M^{n+k} given in [**2**, page 120], which is a consequence of Lemma 1. □

The main results of Belbachir and Bencherif [**3**, Theorem 3, Theorem 4] are contained in the following two propositions:

Proposition 2. *The linear recurrent sequence defined by $x_{-n} = b_n$ for $0 \leq n < m$ and*

$$x_n = \sum_{k=1}^{m} a_k x_{n-k}$$

for $n > 0$, can be written as

$$x_n = \sum_{k=0}^{m-1} c_k y_{n+k},$$
$$-c_k = \sum_{i=k}^{m-1} a_{i-k} b_i \tag{3}$$

for $0 \le k < m$ *with* $a_0 = -1$, *and with*

$$y_n = \sum_{k_1+2k_2+\cdots+mk_m=n} \binom{k_1+\cdots+k_m}{k_1,\ldots,k_m} a_1^{k_1}\cdots a_m^{k_m} \tag{4}$$

for $n > -m$.

Proof. Formula (3) appears in a slightly different notation in [**2**, page 118]. It is also a consequence of Lemma 1. □

Proposition 3. *For* $n > 0$*, the* n*-th power, of an* $m \times m$ *matrix* M *of characteristic polynomial*

$$C_M(x) = x^m - a_1x^{m-1} - \cdots - a_m$$

can be written as

$$M^n = \sum_{k=1}^{m} y_{n-m+k}A_{m-k}$$

where

$$-A_k = \sum_{i=0}^{k} a_iM^{k-i}$$

for $0 \le k < m$ *with* $a_0 = -1$ *and* y_n *being defined by* (4).

Proof. This follows after some computation from the formula for M^{n+k} in Agou's paper [**1**, page 120]. □

4. Proof of Theorem 1

From Lemma 1, by taking $n = 2$, and $k = q-2$, we can write the remainder R of the euclidean division of the monomial $M = x^{q-1}$ by the polynomial $S = x^2-ax-b$ in the form $R = C_1x + D_1$ where

$$t_{q-2,0} = D_1 = \sum_{u+2v=q-1,u\ge 0,v\ge 0} \frac{(u+v-1)!}{u!v!}va^ub^v \tag{5}$$

and

$$t_{q-2,1} = C_1 = \sum_{u+2v=q-2,u\ge 0,v\ge 0} \frac{(u+v-1)!}{u!v!}(u+v)a^ub^v. \tag{6}$$

Observe that with $w = v-1$ the equation (5) becomes

$$t_{q-2,0} = D_1 = \sum_{u+2w=q-3,u\ge 0,w\ge -1} \binom{u+w}{u}a^ub^{w+1} = bD. \tag{7}$$

On the other hand, we see immediately that

$$t_{q-2,1} = C_1 = \sum_{u+2v=q-2, u\geq 0, v\geq 0} \binom{u+v}{u} a^u b^v = C. \tag{8}$$

Setting $x = b$ in the equality

$$M = x^{q-1} = QS + R$$

where Q is the quotient of the euclidean division of M by S and R is the remainder we get

$$b^{q-1} = R(b) = C_1 b + D_1 = Cb + Db$$

since b (and 1) are the roots of the polynomial $S = x^2 + ax + b$. Simplifying by b, we get the result immediately. This proves the theorem.

5. Proof of Theorem 2

Let $m \geq 0$ be a non-negative integer. Let $A \in \mathbb{F}_q[t]$ be any nonzero polynomial. We claim that for any sequence (f_n) defined by $f_m = 0$, $f_{m+1} = A$ and $f_{n+m+1} = f_{n+m} + \Delta f_{n+m-1}$ for all integers $n > 0$, there exists an integer $h > 0$ such that $f_{m+h+1} = 0$.

Assuming the claim we prove that there is an infinity of integers $h > 0$ such that $f_h = 0$. If this is not true, then let $h_0 > 0$ be the largest integer $h > 0$ for which $f_h = 0$. By the claim with $m = h_0$ and $A = f_{h_0+1} \neq 0$, there exists an integer $h_1 > 0$ such that $f_{m+1+h_1} = 0$. Take $h = m + 1 + h_1$. We then have $h > h_0 > 0$ and $f_h = 0$ contradicting the maximality of h_0. This proves that there is an infinity of integers $h > 0$ such that $f_h = 0$.

Now we prove the claim. Assume that for all integers $n > 1$ we have $f_{m+n} \neq 0$. Set $s_0 = 0$, $s_1 = \Delta$, $s_n = \frac{f_{n+m+1}}{f_{n+m}}$ for all integers $n > 1$. Note that this sequence is well defined because we are assuming $f_{n+m} \neq 0$.

Observe that one has

$$s_n(s_{n+1} + 1) = \Delta. \tag{9}$$

Let $x \in F = \overline{\mathbb{F}_q(t)}$, where F is a fixed algebraic closure of the rational field $\mathbb{F}_q(t)$, be such that

$$x^2 + x = \Delta. \tag{10}$$

Since $\Delta \neq 0$, one has $x \notin \{0, 1\}$. We define the sequence $(t_n) \in F$ by $t_n = s_n + x$ for all integers $n > 0$. From the definition of (t_n) and from (9), one has

$$(x + t_n)(x + 1 + t_{n+1}) = \Delta \neq 0. \tag{11}$$

So $t_n \neq x$ for any such n. This is true for all $n > 1$. Thus, $x \notin \{t_n, t_{n+1}\}$.

Now from (11) and (10), one has

$$t_{n+1} = \frac{t_n(x+1)}{t_n + x}. \tag{12}$$

From this, by replacing n by $n+1$ in (12) and using (12) again, we obtain

$$t_{n+2} = \frac{t_{n+1}(x+1)}{t_{n+1}+x} = \frac{t_n(x+1)^2}{t_n x + t_n + x^2 + x t_n} \tag{13}$$

so that

$$t_{n+2} = \frac{t_n(x+1)^2}{t_n + x^2}. \tag{14}$$

If $t_n = x^2$, then from (14) we get $t_n = 0$ since $x \neq 1$. Since $x \neq 0$, one has

$$t_n \neq x^2. \tag{15}$$

But $t_{n+2} \neq x$. Observe that this implies $t_{n+1} \neq x^2$ since from

$$t_{n+2} = \frac{t_{n+1}(x+1)}{t_{n+1}+x}$$

we get $t_{n+2} = x$ if $t_{n+1} = x^2$. Now, in order to obtain t_{n+3} we have two possible paths. The first one is to replace n by $n+2$ in (12) and use (14). This gives

$$t_{n+3} = \frac{t_{n+2}(x+1)}{t_{n+2}+x} = \frac{t_n(x+1)^3}{t_n(x+1)^2 + x^2(t_n + x^2)} \tag{16}$$

$$t_{n+3} = \frac{t_n(x+1)^3}{t_n + x^4}. \tag{17}$$

The second path is to replace n by $n+1$ in (14) and use (12). This gives

$$t_{n+3} = \frac{t_{n+1}(x+1)^2}{t_{n+1}+x^2} = \frac{t_n(x+1)^3}{t_n(x+1) + x^2(t_n + x)} \tag{18}$$

so that we get

$$t_{n+3} = \frac{t_n(x+1)^3}{t_n(x^2+x+1) + x^3}. \tag{19}$$

So from (17) and (19), we obtain

$$t_n x(x+1) = x^3(x+1). \tag{20}$$

Recall that $x \notin \{0, 1\}$. Thus, from (20) we get

$$t_n = x^2. \tag{21}$$

But (21) contradicts (15). This proves the claim, thereby proving the theorem.

Acknowledgment. The authors are grateful to the referee for careful reading and detailed suggestions. The result is an improved paper. An interesting question of the referee concerns the possible periodicity of the linear sequence considered in this paper. We do not know how to answer the question, but this encourages us to do more work on this area.

References

1. Agou S., *Sur les formules explicites intervenant dans la division euclidienne des polynômes et leurs conséquences.* C. R. Acad. Sci. Paris Ser. A-B **273** (1971), A209–A211

2. ______, *Formules explicites intervenant dans la division euclidienne des polynômes à coefficients dans un anneau unitaire et applications diverses.* Publ. Dép. Math. (Lyon) **8(1)** (1971), 107–121.

3. Belbachir H. and Bencherif F., *Linear recurrent sequences and powers of a square matrix.* Integers **6** (2006), A12, 17pp.

4. Cherly J., Gallardo L., Vaserstein L. and Wheland E., *Solving quadratic equations over polynomial rings of characteristic two.* Publ. Mat. **42(1)** (1998), 131–142.

5. Gallardo L., Vaserstein L. and Wheland E., *Berlekamp's discriminant and cubic equations in characteristic two.* JP J. Algebra Number Theory Appl. **3(2)** (2003), 169–178.

6. Hardy G. H. and Wright E. M., *An introduction to the theory of numbers*, 4th Edit. Oxford, Clarendon Press, 1960.

7. McLaughlin J., *Combinatorial identities deriving from the n-th power of a 2×2 matrix.* Electronic Journal of Combinatorial Number Theory **4** (2004), A19.

R. Euler, Computer Science, University of Brest, 20, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France, *e-mail*: `Reinhardt.Euler@univ-brest.fr`

L. H. Gallardo, Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France, *e-mail*: `Luis.Gallardo@univ-brest.fr`