JOURNAL OF NUMBER THEORY 27, 144–148 (1987)

Continued Fraction Expansions of Rational Expressions with Irreducible Denominators in Characteristic 2

JILL P. MESIROV*

American Mathematical Society, Providence, Rhode Island 02940

AND

MELVIN M. SWEET

The Aerospace Corporation, Computer Sciences Laboratory, P. O. Box 92957, Los Angeles, California 90009

Communicated by H. Stark

Received January 10, 1985; revised January 2, 1986

Given any irreducible polynomial q of degree n over the field with two elements, there is a sequence of polynomials $p_n, p_{n-1}, \ldots, p_0$ with $p_n = q$, with $p_0 = 1$, with the degree of p_i equal to i, and with $p_i \equiv p_{i-2} \pmod{p_{i-1}}$. In other words, given an irreducible q there is a p, relatively prime to q, with degree one less and such that the degrees of the remainders in Euclid's Algorithm for the greatest common divisor of p and q go down by exactly 1 at each step. © 1987 Academic Press, Inc.

STATEMENT OF RESULTS

Let F be the finite field with two elements, and let K be the field $F((x^{-1}))$ of all formal power series in x^{-1} over F. Every element f of K has a continued fraction expansion $f = a_0 + 1/(a_1 + 1/(a_2 + \cdots))$ which we denote by $f = [a_0; a_1, a_2, \ldots]$ (see Sect. 1 of [1] for a discussion of the continued fraction theory for K). The elements of K which are in the field of rational functions, $F(x)$, have finite continued fraction expansions; these are the elements we will be concerned with in this paper. We will show that for every irreducible polynomial q over F with degree n, there is a polynomial p with degree $< n$ for which the partial quotients of the continued fraction expansion $[0; a_1, a_2, \ldots, a_m]$ of p/q all have degree one (so $m = n$). In fact, we will show that for each irreducible denominator, q, there are exactly two

* Current address: Thinking Machines Corporation, 245 First St., Cambridge, MA 02142.

0022-314X/87 $3.00

such numerators. This result is equivalent to the following: Given any irreducible polynomial q of degree n over F, there is a sequence of polynomials $p_n, p_{n-1}, \ldots, p_0$ with $p_n = q$, with $p_0 = 1$, with the degree of p_i equal to i, and with $p_i \equiv p_{i-2} \pmod{p_{i-1}}$. In other words, given q there is a p such that the degrees of the remainders in Euclid's Algorithm for the greatest common divisor of p and q go down by exactly 1 at each step.

The proof uses results of Baum and Sweet [2], and it can be modified to prove the following. Suppose that q has m distinct irreducible factors different from x and $x+1$. If there is a polynomial p for which $p/q = [0; a_1, \ldots, a_n]$ with degree $(a_i) = 1$ for all i, then there are 2^m such p. For example, $q = x(x^2+x+1)^2(x^3+x+1)$ has 4 polynomials p if it has one.

We wish to thank Dave Robbins at the Institute for Defense Analyses in Princeton. The present result was suggested during discussions with him about our conjecture that every polynomial is the denominator of an expression p/q which has partials quotients of degree 1 or 2. This more general conjecture (for non-irreducible q) is still open.

Proof

In this section we establish the result, by showing that given an irreducible q over F with degree n there is a polynomial p for which the partial quotients of p/q all have degree 1. For a candidate numerator p, write

$$p/q = f_1 x^{-1} + f_2 x^{-2} + \cdots + f_k x^{-k} + \cdots.$$

Note that the binary sequence $f_1, f_2, \ldots$ satisfies the recursion q, i.e., if $q = x^n + q_{n-1}x^{n-1} + \cdots + q_0$, then

$$f_{n+i} = q_{n-1}f_{n-1+i} + q_{n-2}f_{n-2+i} + \cdots + q_0 f_i, \qquad i \geqslant 1. \tag{1}$$

From the remark on p. 577 of [2] all partial quotients a_i will have degree one if

$$\begin{aligned} f_1 &= 1 \\ f_i + f_{2i} + f_{2i+1} &= 0 \qquad \text{for } i = 1, 2, \ldots, n-1 \\ f_n + f_{2n} + f_{2n+1} &= 1 \end{aligned} \tag{2}$$

and, of course, the f_i satisfy the recursion q. We will use the following lemma to reduce these to linear equations involving only the initial variables $f_1, f_2, \ldots, f_n$:

LEMMA. *Let $b_1, b_2, ..., b_d$ be in F. Then*

$$\sum_{i=1}^{d} b_i x^{i-1} \equiv 0 \pmod{q}$$

if and only if for all 2^n initial choices of $f_1, f_2, ..., f_n$ in the recursion (1) *we have*

$$\sum_{i=1}^{d} b_i f_i = 0.$$

(The proof is by induction on d and does not require that q be irreducible.)

Now consider the $n+1$ by n matrix A obtained by reducing the $n+1$ polynomials

$$x^0, x^{i-1} + x^{2i-1} + x^{2i} \qquad \text{for } i = 1, 2, ..., n \tag{3}$$

modulo q. Using the lemma, we see that solving (2) is equivalent to solving the linear system

$$Av = (1, 0, 0, ..., 0, 1)^t \tag{4}$$

where $v = (f_1, ..., f_n)^t$, and where the exponent t stands for transpose Thus the rational expression p/q will have degree one partial quotients if there exists a solution vector v to Eq. (4). The f_i for $i > n$ are obtained from v by applying the recursion in Eq. (1).

Let B be the n by n matrix consisting of the last n rows of A. The polynomial corresponding to the ith row of b is

$$x^{i-1} + x^{2i-1} + x^{2i} \pmod{q}.$$

Therefore, again by the lemma, it follows that the matrix equation

$$uB = 0$$

is equivalent to the congruence

$$r(x) + xr(x)^2 + x^2 r(x)^2 \equiv 0 \pmod{q},$$
$$\text{where } r(x) = u_1 + u_2 x + \cdots + u_n x^{n-1},$$

since $r(x)^2 = r(x^2)$. This congruence has a unique non-zero solution because we are assuming that q is irreducible. The solution is the inverse of $x(x+1)$ modulo q. Thus the row rank of B is $n-1$.

Similarly by the lemma, the matrix equation

$$wA = 0, \qquad w_1 = 1$$

corresponds to the congruence

$$r(x) + xr(x)^2 + x^2 r(x)^2 \equiv 1 \pmod{q},$$

or equivalently

$$1 + r(x) + x(x+1)\, r(x)^2 = (1 + xr(x))(1 + (x+1)\, r(x)) \equiv 0 \pmod{q}.$$

Again, since q is irreducible, this polynomial has exactly two distinct solutions. So there are exactly two solutions w^1, w^2 of $wA = 0$ with $w_1 = 1$. The two solutions come from $xr(x) \equiv 1 \pmod{q}$ and $(x+1)\, r(x) \equiv 1 \pmod{q}$, and therefore must have the coefficient of x^{n-1} in $r(x)$ non-zero. So $w^1_{n+1} = w^2_{n+1} = 1$. The solution $w^1 + w^2$ is thus non-trivial and does not involve the first or last row of A. Thus these middle rows are dependent and, since the rank of B is $n-1$, the last row of B is independent of the other rows. This means that if we adjoin the column $(0, 0, ..., 0, 1)^t$ to B then the row rank, and therefore also the column rank, does not change. Therefore the system

$$Bv = (0, 0, ..., 0, 1)^t$$

has two solutions. Because we know the first row of A is the sum of the last row of B and some other rows of B, these solutions are also solutions of

$$Av = (1, 0, 0, ..., 0, 1)^t.$$

This shows the existence of two numerators, p, as claimed.

We now give a simple example. Take $q = x^5 + x^3 + x^2 + x + 1$ which is irreducible over F. The matrix A found by reducing equations (3) is

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

This matrix does indeed have rank 4. The two solutions of Eq. (4) are $(f_1, f_2, f_3, f_4, f_5) = (1, 0, 1, 0, 0)$ and $(f_1, f_2, f_3, f_4, f_5) = (1, 1, 0, 0, 1)$. These correspond to the polynomials $p_1 = x^4 + x$ and $p_2 = x^4 + x^3 + x^2 + 1$ which can be found by multiplying q by $f_1 x^{-1} + f_2 x^{-2} + f_3 x^{-3} + f_4 x^{-4} + f_5 x^{-5}$ and taking only non-negative powers of x. We have $p_1/q = [0; x, x, x, x+1, x+1]$ and $p_2/q = [0; x+1, x+1, x, x, x]$. Note that the continued fraction expansion for p_1/q is the expansion for p_2/q backwards. This is always true for the two solutions and is an elementary continued

fraction result. If we take the continued fraction expansion for any other p then at least one partial quotient will have degree larger than 1, for example, if $p = x^4 + 1$ then $p/q = [0; x, x + 1, x, x^2 + x]$.

REFERENCES

1. L. E. BAUM AND M. M. SWEET, Continued fractions of algebraic power series in characteristic 2, *Ann. of Math.* **103** (1976).
2. L. E. BAUM AND M. M. SWEET, Badly approximable power series in characteristic 2, *Ann. of Math.* **105** (1977), 573–580.