Canad. Math. Bull. Vol. **17** (2), 1974

NOTE ON A PAPER OF S. UCHIYAMA

BY
B. C. MORTIMER AND K. S. WILLIAMS

Let p be a rational prime and n a positive integer ≥ 2. We denote by $a_n(p)$ the least positive integral value of a for which the polynomial x^n+x+a is irreducible (mod p), and set

(1) $$a_n = \liminf_{p\to\infty} a_n(p).$$

One of us (K. S. W. [4]) conjectured that $a_n=1$ for all $n\geq 2$. As has been pointed out by Uchiyama (and others) this is not true when $n\equiv 2 \pmod 3$ and $n>2$, since then x^n+x+1 has the factor x^2+x+1 in $Z[x]$ and so $a_n\geq 2$ in this case. However, it was proved in [4] that $a_2=a_3=1$ and Uchiyama [3] has considered a_n for $n\leq 10$. Implicit in Uchiyama's paper is the following theorem:

THEOREM 1. *Let a_n^* be the least positive integer a such that there exists some prime p_n for which x^n+x+a is irreducible mod p_n. Then $a_n=a_n^*$.*

Using this theorem Uchiyama deduced that

$$a_2 = a_3 = a_4 = a_6 = a_7 = a_9 = a_{10} = 1, \qquad a_5 = 3, \qquad a_8 = 2.$$

However, doubt is cast on two of these values as Uchiyama's paper contains two errors. First of all x^8+x+2 is not irreducible (mod 3) as claimed by him since

$$x^8+x+2 \equiv (x^3+2x^2+2x+2)(x^5+x^4+2x^3+x^2+x+1) \pmod 3,$$

thus $a_8=2$ is *not* established. Secondly $x^{10}+x+1$ is not irreducible (mod 2) since

$$x^{10}+x+1 \equiv (x^3+x+1)(x^7+x^5+x^4+x^3+1) \pmod 2,$$

thus $a_{10}=1$ is *not* established. In this note we review a_n for $2\leq n\leq 10$ and also consider a_n for $11\leq n\leq 20$.

The following lemma eliminates cases where x^n+x+a is reducible in $Z[x]$.

LEMMA.

$$a_n^* \geq 2, \qquad \text{if } n \equiv 2 \pmod 6, \qquad n > 2,$$
$$a_n^* \geq 3, \qquad \text{if } n \equiv 5 \pmod 6.$$

Proof. This is clear for if $n\equiv 2 \pmod 6$, $n>2$, then x^n+x+1 is divisible by x^2+x+1 in $Z[x]$; and if $n\equiv 5 \pmod 6$ then x^n+x+1 is divisible by x^2+x+1 in $Z[x]$ and x^n+x+2 is divisible by $x+1$ in $Z[x]$.

Factorizations of x^n+x+a modulo a prime were accomplished using an algorithm due to Berlekamp [1]. In this algorithm, in order to factor $x^n+x+a \pmod p$, a polynomial $g(x)$ is determined such that $(g(x))^p \equiv g(x)$ (modulo x^n+x+a). It is shown in [1] that for such a polynomial $g(x)$ we have

$$x^n+x+a = \prod_{0 \leq s < p} \text{G.C.D.}(x^n+x+a,\ g(x)-s),$$

and this factorization is non-trivial if and only if $\deg(g(x))>0$. The coefficients of all such possible polynomials $g(x)$ arise as the eigenvectors of the $n \times n$ matrix whose ith row consists of the coefficients of $x^{(i-1)p}$ reduced modulo x^n+x+a. Calculations were performed on Carleton University's Xerox Data Systems Sigma 6 computer and the following table gives the resulting values of a_n^* for $2 \leq n \leq 20$.

From this table, the lemma and theorem 1, we obtain

THEOREM 2.

$$a_n = 1, \quad \text{for } n = 2, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 18, 19,$$
$$a_n = 2, \quad \text{for } n = 8, 14, 20,$$
$$a_n = 3, \quad \text{for } n = 5, 11, 17.$$

This suggests the following possible modification of the original ill-fated conjecture of [4] (the first line of which has been conjectured by Uchiyama):

CONJECTURE. For $n \geq 3$,

$$a_n = \begin{cases} 1, & \text{if } n \equiv 0, 1 \pmod 3, \\ 2, & \text{if } n \equiv 2 \pmod 6, \\ 3, & \text{if } n \equiv 5 \pmod 6. \end{cases}$$

The work of Uchiyama [3] shows that this conjecture is true whenever n is an odd prime. From the work of Zierler [2] we see that it is also true for

$$n = 22, 28, 30, 46, 60, 63, 153, 172, 303, 471, 532, 865, 900, 1366, 2380, 3310, 4495, 6321, 7447, 10198, 11425, 21846, 24369, 27286, 28713.$$

(Added in proof) Prof. M. Sato (Kyoto University) and Prof. M. Yorinaga (Okayama University) have now verified our conjecture for the remaining values of $n \leq 40$.

REFERENCES

1. E. R. Berlekamp, *Algebraic coding Theory*, McGraw-Hill Book Company (1968), Chapter 6.
2. N. Zierler, *On x^n+x+1 over GF(2)*, Information and Control **16** (1970), 502–505.
3. S. Uchiyama, *On a conjecture of K. S. Williams*, Proc. Japan Acad. **46** (1970), 755–757.
4. K. S. Williams, *On two conjectures of Chowla*, Canad. Math. Bull. **12** (1969), 545–565.

CARLETON UNIVERSITY,
OTTAWA, CANADA

n	polynomial	p	reducibility (mod p)	a_n^*
2	x^2+x+1	2	irreducible	1
3	x^3+x+1	2	irreducible	1
4	x^4+x+1	2	irreducible	1
5	x^5+x+3	2	factor x^2+x+1	
		3	factor x	
		5	factor $x+4$	
		7	irreducible	3
6	x^6+x+1	2	irreducible	1
7	x^7+x+1	2	irreducible	1
8	x^8+x+2	2	factor x	
		3	factor x^3+2x^2+2x+2	
		5	factor $x+3$	
		7	factor $x+4$	
		11	factor $x+6$	
		13	factor $x+11$	
		17	irreducible	2
9	x^9+x+1	2	irreducible	1
10	$x^{10}+x+1$	2	factor x^3+x+1	
		3	factor $x+2$	
		5	factor x^2+4x+2	
		7	factor x^2+6x+6	
		11	factor $x+2$	
		13	factor $x+11$	
		17	factor $x^3+13x^2+8x+11$	
		19	factor $x+10$	
		23	factor $x^2+13x+20$	
		29	factor $x+15$	
		31	factor $x+2$	
		37	factor $x+22$	
		41	factor $x^5+2x^4+x^3-5x^2-2x+12$*	
		43	factor $x+18$	
		47	factor $x^2+3x+30$	
		53	factor $x+5$	
		59	factor $x^3+37x^2+36x+1$	
		61	factor $x^2+54x+5$	
		67	factor $x+50$	
		71	factor $x^2+50x+23$	
		73	irreducible	1

* (Added in proof) Inadvertently the authors overlooked the reducibility of $x^{10}+x+1$ (mod 41). The given factor was obtained by Mr. M. Andô in Nagoya and kindly communicated to us by Prof. M. Sato of Kyoto University.

n	polynomial	p	reducibility (mod p)	a_n^*
11	$x^{11}+x+3$	2	factor x^2+x+1	
		3	factor x	
		5	factor $x+4$	
		7	irreducible	3
12	$x^{12}+x+1$	2	factor $x^5+x^3+x^2+x+1$	
		3	factor $x+2$	
		5	factor $x+2$	
		7	factor $x+2$	
		11	factor $x^3+x^2+9x+10$	
		13	factor $x+2$	
		17	factor $x+5$	
		19	irreducible	1
13	$x^{13}+x+1$	2	factor $x^5+x^4+x^3+x+1$	
		3	factor $x+2$	
		5	factor $x+3$	
		7	factor $x+4$	
		11	factor $x+9$	
		13	factor $x+7$	
		17	factor $x+11$	
		19	irreducible	1
14	$x^{14}+x+2$	2	factor x	
		3	irreducible	2
15	$x^{15}+x+1$	2	irreducible	1
16	$x^{16}+x+1$	2	factor $x^8+x^6+x^5+x^3+1$	
		3	factor $x+2$	
		5	factor $x+2$	
		7	factor $x^4+6x^3+4x^2+5x+3$	
		11	factor $x+6$	
		13	factor $x^2+12x+12$	
		17	factor $x+2$	
		19	factor $x^4+9x^3+3x^2+12$	
		23	factor $x+9$	
		29	factor $x^4+16x^3+8x^2+9x+23$	
		31	factor $x^4+15x^3+19x^2+17x+6$	
		37	factor $x+17$	
		41	factor $x+11$	
		43	factor $x^2+15x+35$	
		47	factor $x+17$	
		53	factor $x^2+33x+7$	
		59	factor $x+49$	
		61	factor $x^7+6x^6+18x^5+37x^4+38x^3+8x^2+43x+50$	
		67	factor $x^3+21x^2+54x+55$	
		71	factor $x^2+37x+63$	
		73	factor $x+33$	
		79	irreducible	1

n	polynomial	p	reducibility (mod p)	a_n^*
17	$x^{17}+x+3$	2	factor x^2+x+1	
		3	factor x	
		5	factor $x+4$	
		7	irreducible	3
18	$x^{18}+x+1$	2	factor x^5+x^2+1	
		3	factor $x+2$	
		5	irreducible	1
19	$x^{19}+x+1$	2	factor x^4+x+1	
		3	factor $x+2$	
		5	factor x^3+3x^2+2x+3	
		7	factor x^3+3x^2+3x+4	
		11	factor $x^7+4x^6+x^5+8x^4+10x^3+10x^2+2x+5$	
		13	factor x^4+7x^3+7x+4	
		17	factor $x+6$	
		19	factor $x+10$	
		23	factor $x+6$	
		29	factor $x+27$	
		31	factor $x^5+21x^4+26x^3+13x^2+20x+15$	
		37	factor x^3+5x^2+6x+1	
		41	factor $x+7$	
		43	factor $x+26$	
		47	factor $x^2+41x+21$	
		53	factor $x+44$	
		59	irreducible	1
20	$x^{20}+x+2$	2	factor x	
		3	factor $x^5+2x^3+x^2+x+2$	
		5	factor $x+3$	
		7	factor $x+4$	
		11	factor $x+3$	
		13	factor $x+11$	
		17	factor $x+6$	
		19	irreducible	2