172. *Numerical Experiments on a Conjecture of B. C. Mortimer and K. S. Williams*

By Masahiko SATO*) and Masataka YORINAGA**)

(Comm. by Kenjiro SHODA, M. J. A., Dec. 12, 1973)

Let p be a rational prime and n a positive integer $\geqq 2$. 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

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

B. C. Mortimer and K. S. Williams [2] have stated the following

Conjecture. *Put* $a_2^*=1$ *and for* $n\geqq 3$ *define*

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

Then we have $a_n=a_n^*$.

K. S. Williams [5] proved that this conjecture is in fact true for $n=2$ and 3, and Mortimer and Williams [2] verified the conjecture for all $n\leqq 20$ with the aid of a computer. The results of S. Uchiyama [4] show that the conjecture is true whenever n itself is a prime number.

In § 1 of the present paper we shall show that the conjecture is true for all $n\leqq 40$ by making use of an algorithm which is *faster* than the one used in [2]. As to the discriminant D_n of the polynomial $x_n+x+a_n^*$, it is possible to examine the values of it for a fairly wider range of n, and we observe in § 2 some arithmetical properties of D_n that will be of an independent interest. The computations in § 1 were accomplished by the first-named author and those in § 2 were done by the second-named author.

The authors wish to express here their sincerest thanks to Prof. S. Hitotumatu and Prof. S. Uchiyama for the valuable suggestions.

§ 1. Irreducibility of $x^n+x+a_n^*$ (mod p). Our basic tool is as in [4] the following theorem which is an immediate consequence of the Frobenius density theorem (cf. [1; Chap. IV, § 5]).

Theorem 1. *Let* $n\geqq 2$. *If there exists some prime* p *such that* $f_n(x)=x^n+x+a_n^*$ *is irreducible* (mod p), *then* $a_n=a_n^*$.

Thus, if we can find some prime p such that $f_n(x)$ is irreducible (mod p), then the conjecture of Mortimer and Williams is true for this n. Our algorithm is based on the following three theorems.

*) Department of Mathematics, Kyoto University, Kyoto.
**) Department of Mathematics, Okayama University, Okayama.

Theorem 2. *Let D_n denote the discriminant of $f_n(x)$. Then*

$$D_n=(-1)^{n(n-1)/2}(n^n a_n^{*n-1}+(-1)^{n-1}(n-1)^{n-1}).$$

For a proof of this and the next theorems we refer to R. G. Swan [3].

Theorem 3. *Let p be an odd prime, and $f(x)$ be a monic polynomial of degree n over $GF(p)$, with discriminant $D\neq 0$. Let r be the number of irreducible factors of $f(x)$ over $GF(p)$. Then $r\equiv n \pmod 2$ if and only if D is a square in $GF(p)$.*

Theorem 4. *Let p be a prime, and $f(x)$ be a polynomial of degree n over $GF(p)$. Then $f(x)$ is irreducible over $GF(p)$ if and only if the greatest common divisor $\mathrm{GCD}(f(x), x^{p^m}-x)=1$ for all m satisfying $1<2m\leqq n$.*

Proof. Suppose that $f(x)$ is irreducible over $GF(p)$, and that $\mathrm{GCD}\,(f(x), x^{p^m}-x)=1$ for some $m, 1\leqq m<n$. Then $f(x)\,|\,x^{p^m}-x$, and we must have $GF(p^n)\subset GF(p^m)$. This is apparently a contradiction.

Suppose now that $f(x)$ is reducible over $GF(p)$. Then $f(x)$ has an irreducible factor $g(x)$ of degree $m\leqq n/2$. Clearly, $g(x)\,|\,x^{p^m}-x$. Hence $\mathrm{GCD}\,(f(x), x^{p^m}-x)\neq 1$.

By making use of the above theorems, we wrote down a Fortran program to find the least prime p which satisfies the condition in

Table I

n	$f_n(x)=x^n+x+a_n^*$	p_n	n	$f_n(x)=x^n+x+a_n^*$	p_n
2	x^2+x+1	2	21	$x^{21}+x+1$	281
3	x^3+x+1	2	22	$x^{22}+x+1$	2
4	x^4+x+1	2	23	$x^{23}+x+3$	113
5	x^5+x+3	7	24	$x^{24}+x+1$	227
6	x^6+x+1	2	25	$x^{25}+x+1$	101
7	x^7+x+1	2	26	$x^{26}+x+2$	337
8	x^8+x+2	17	27	$x^{27}+x+1$	5
9	x^9+x+1	2	28	$x^{28}+x+1$	2
10	$x^{10}+x+1$	73	29	$x^{29}+x+3$	89
11	$x^{11}+x+3$	7	30	$x^{30}+x+1$	2
12	$x^{12}+x+1$	19	31	$x^{31}+x+1$	5
13	$x^{13}+x+1$	19	32	$x^{32}+x+2$	463
14	$x^{14}+x+2$	3	33	$x^{33}+x+1$	7
15	$x^{15}+x+1$	2	34	$x^{34}+x+1$	619
16	$x^{16}+x+1$	79	35	$x^{35}+x+3$	193
17	$x^{17}+x+3$	7	36	$x^{36}+x+1$	229
18	$x^{18}+x+1$	5	37	$x^{37}+x+1$	587
19	$x^{19}+x+1$	59	38	$x^{38}+x+2$	137
20	$x^{20}+x+2$	19	39	$x^{39}+x+1$	11
			40	$x^{40}+x+1$	199

Theorem 1. The computations were done on a TOSBAC 3400 at the Research Institute for Mathematical Sciences, Kyoto University, and on a HITAC 8700 at the Institute of Statistical Mathematics, Tokyo. Table I shows that the conjecture is true for all $n \leqq 40$. In the table p_n denotes the least prime p such that $f_n(x)$ is irreducible (mod p).

§ 2. Numerical observations on D_n. In the following our main interest is in computing values of the discriminant D_n of the polynomial $f_n(x) = x^n + x + a_n^*$ and in examining the complete squareness of D_n.

Actually we computed D_n in its own value and sought for its square root by means of a multi-precisions' procedure, within the limit of integers as far as $n \leqq 112$. And then, for n exceeding this limit, we prefered to compute D_n by reducing with modulus p for each of 24 prime numbers p, $3 \leqq p \leqq 97$, in succession, until D_n turned to appear as a quadratic non-residue (mod p).

In such a manner, we executed the computations for $n \equiv 0, 1$ (mod 4), $n \leqq 32765$, and we found that for each of these n there always exists a prime p such that D_n is a quadratic non-residue (mod p). (Note that, by Theorem 2, $D_n > 0$ when and only when $n \equiv 0$ or 1 (mod 4).) We thus have the following

Conclusion. *The discriminant D_n of the polynomial $f_n(x)$ is not a complete square number for all $n \leqq 32765$.*

As a by-product of the above computations we observed the fact that for each of the primes p referred to there is a periodicity modulo p in the sequence D_n ($n = 2, 3, 4, \cdots$), as shown in Table II. Moreover, the (smallest possible) period N_p of the sequence D_n (mod p) was found

Table II

p	$p-1$	N_p
3	2	$4 = 2^2$
5	2^2	$60 = 2^2 3 \cdot 5$
7	$2 \cdot 3$	$84 = 2^2 3 \cdot 7$
11	$2 \cdot 5$	$660 = 2^2 3 \cdot 5 \cdot 11$
13	$2^2 3$	$156 = 2^2 3 \cdot 13$
17	2^4	$816 = 2^4 3 \cdot 17$
19	$2 \cdot 3^2$	$684 = 2^2 3^2 19$
23	$2 \cdot 11$	$3036 = 2^2 3 \cdot 11 \cdot 23$
29	$2^2 7$	$2436 = 2^2 3 \cdot 7 \cdot 29$
31	$2 \cdot 3 \cdot 5$	$1860 = 2^2 3 \cdot 5 \cdot 31$
37	$2^2 3^2$	$1332 = 2^2 3^2 37$
41	$2^3 5$	$4920 = 2^3 3 \cdot 5 \cdot 41$
43	$2 \cdot 3 \cdot 7$	$3612 = 2^2 3 \cdot 7 \cdot 43$
47	$2 \cdot 23$	$12972 = 2^2 3 \cdot 23 \cdot 47$

to be the least common multiple, LCM $(12, p(p-1))$, except for the case of $p=3$. It will be readily verified that the period N_p must in general be a divisor of LCM $(12, p(p-1))$.

The computations were performed on a HITAC 10 in the Department of Mathematics, Okayama University.

§3. A remark. In the factor table of $f_n(x) \pmod p$ given by Mortimer and Williams [2], there is a slip of a row corresponding to the decomposition of $f_{10}(x) \pmod{41}$. Quite recently, this lack has been supplied by Mr. M. Andô in Nagoya, who found that

$$f_{10}(x) \equiv (x^5+2x^4+x^3-5x^2-2x+12) \cdot (x^5-2x^4+3x^3+x^2-13x+24) \pmod{41},$$

the each of the two factors on the right being irreducible (mod 41). It is reported that the relevant computation was done on a computer, FACOM 230–25.

This remark is due to Prof. Hitotumatu.

References

[1] G. J. Janusz: Algebraic Number Fields. Academic Press, New York and London (1973).

[2] B. C. Mortimer and K. S. Williams: Note on a paper of S. Uchiyama (to appear).

[3] R. G. Swan: Factorization of polynomials over finite fields. Pacific J. Math., **12**, 1099–1106 (1962).

[4] S. Uchiyama: On a conjecture of K. S. Williams. Proc. Japan Acad., **46**, 755–757 (1970).

[5] K. S. Williams: On two conjectures of Chowla. Canad. Math. Bull., **12**, 545–565 (1969).