

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 ≥ 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

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

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

Conjecture. Put $a_2^* = 1$ and for $n \geq 3$ 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 $n \leq 20$ 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 $n \leq 40$ 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 $n \geq 2$. 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.