173. *On a Conjecture of K. S. Williams*

By Saburô UCHIYAMA
Department of Mathematics, Shinshû University, Matsumoto
(Comm. by Kinjirô KUNUGI, M. J. A., Sept. 12, 1970)

1. 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 which makes the polynomial x^n+x+a irreducible (mod p). In a recent paper [3] K. S. Williams conjectured that for all $n \geqq 2$ one has

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

and showed (among others) that (1) is true for $n=2$ and 3. In the present note we shall prove that (1) is true for $n=4$, 6, 9, 10 and for all primes $n\equiv 1 \pmod 3$. However, it is immediately clear that (1) is not true for some (in fact, infinitely many) values of n. Indeed, the polynomial x^n+x+1 is irreducible in $Z[x]$*) if and only if $n=2$ or $n\not\equiv 2$ (mod 3), and for $n\equiv 2 \pmod 3$ x^n+x+1 has the obvious factor x^2+x+1 (cf. [2]). Thus, we can show that for $n=5$

(2) $$\liminf_{p\to\infty} a_5(p)=3$$

and for $n=8$

(3) $$\liminf_{p\to\infty} a_8(p)=2.$$

2. Our foundation is on the following important theorem due to F. G. Frobenius [1].

Theorem. *Let $f(x)$ be a square-free polynomial* (i.e. *a polynomial with non-zero discriminant*) *of degree $n\geqq 1$ in $Z[x]$, and let $d_1, \cdots, d_r$ ($r\geqq 1$) be positive integers with $d_1+\cdots+d_r=n$. Then, if the Galois group of $f(x)$, as a permutation group on n letters, contains a permutation which is decomposed as the product of r cycles of length $d_1, \cdots, d_r$, there are infinitely many primes p such that we have*

(4) $$f(x)\equiv f_1(x)\cdots f_r(x) \pmod p,$$

where $f_1(x), \cdots, f_r(x)$ are polynomials of $Z[x]$, each irreducible (mod p), *of degree $d_1, \cdots, d_r$, respectively.*

In fact, it is proved in [1] that the Dirichlet density of prime numbers p for which (4) holds equals the number of permutations in the Galois group of $f(x)$ that have r cycles of length $d_1, \cdots, d_r$, divided by the order of the group.

By virtue of this theorem, a simple and well-known argument on the reduction (mod p) of the Galois group of $f(x)$ will show that the

---

*) We denote by Z, as usual, the ring of rational integers.