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

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

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 $n\equiv 1$ (mod 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 $n\equiv 2$ (mod 3) x^n+x+1 has the obvious factor x^2+x+1 (cf. [2]). Thus, we can show that for $n=5$

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

and for $n=8$

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

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*

$$(4) \qquad f(x)\equiv f_1(x)\cdots f_r(x) \qquad (\mathrm{mod}\ p),$$

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.

existence of infinitely many primes p satisfying (4) is equivalent to the existence of at least one such prime p (not dividing the discriminant of $f(x)$).

The following result is a particular case of the above theorem.

Corollary. *Let $f(x)$ be a polynomial of degree $n \geqq 1$ in x with coefficients in Z. If the Galois group of $f(x)$ contains a cycle of length equal to n, then there are infinitely many primes p for which $f(x)$ is irreducible* (mod p) (*so that $f(x)$ is necessarily irreducible in $Z[x]$*).

Another interesting consequence of the theorem of Frobenius is that if $f(x)$ is an irreducible polynomial of degree $n \geqq 2$ in $Z[x]$, then there exists an infinity of primes p such that the congruence

$$f(x) \equiv 0 \pmod{p} \tag{5}$$

has no solution x in Z. On the other hand, it is not difficult to see that for an arbitrary non-constant polynomial $f(x)$ in $Z[x]$ there are infinitely many primes p for which the congruence (5) has solutions x in Z.

3. Now, we shall apply the corollary to the theorem of Fobenius, to the special polynomials x^n+x+a, $a \in Z$. The polynomial x^n+x+1 is irreducible in $Z[x]$ for $n \equiv 1$ (mod 3). Hence, if $n \equiv 1$ (mod 3) is prime, then there are infinitely many primes p for which x^n+x+1 is irreducible (mod p). In order to obtain the other results enunciated in § 1, it will suffice to find the least positive value of a and an appropriate prime number p such that x^n+x+a is irreducible (mod p). Thus, the polynomial x^n+x+1 is irreducible (mod 2) for $n=2, 3, 4, 6, 9$ and 10. Hence, (1) holds true for these values of n. Next, we see that the polynomial x^5+x+3 is irreducible (mod 7), so that (2) holds. Finally, the polynomial x^8+x+2 is irreducible (mod 3) and (3) holds.

Also, we can argue for the case of $n=6$ in the following way. We find that

$$x^6+x+1 \equiv (x+2)(x^2+2x+2)(x^3+2x^2+x+1) \pmod{3}$$

and

$$x^6+x+1 \equiv (x+2)(x^5+5x^4+4x^3+6x^2+2x+4) \pmod{7},$$

the factors on the right-hand side being irreducible to the respective moduli. It follows from this that the Galois group of x^6+x+1 is the symmetric group of degree 6. (Here, use was made of the elementary fact that, if a transitive permutation group on n letters contains a transposition and a cycle of length $n-1$, then the group coincides with the symmetric group of degree n.) Thus, the density of prime numbers p for which x^6+x+1 is irreducible (mod p) is equal to $1/6$.

Our method could of course be extended to treat the case of $n>10$, unless we avoided the incleasing complication with n in the reduction of the relevant polynomials with various moduli (except for primes $n \equiv 1$ (mod 3)).

Added in proof (September 21, 1970). It is not difficult to see that the polynomial x^n+x+a, $a\in Z$, is irreducible in $Z[x]$ for $a=3$ and $n\geqq 2$ (for $a=2$ and even $n\geqq 2$). We thus have, in particular,

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

for every odd prime $n\equiv 2 \pmod 3$.

References

[1] F. G. Frobenius: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. Sitzungsberichte Kön. Preuss. Akad. Wiss. Berlin, 689–703 (1896).

[2] E. S. Selmer: On the irreducibility of certain trinomials. Math. Scand., **4**, 287–302 (1956).

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