ON A CERTAIN CONJECTURE OF K. WILLIAMS

MATHEMATICS

1969

SovietRxiv

Abstract

Full Text

UDC 511.22

MATHEMATICS

G. I. PERELMUTER

ON A CERTAIN CONJECTURE OF K. WILLIAMS

(Presented by Academician Yu. V. Linnik, May 13, 1968)

In the paper ([1]) the conjecture was put forward that the pair $(m, m+1)$ of least consecutive residues modulo a prime p of any integer polynomial of degree d satisfies the inequality

$$1 \leq m < C\sqrt{p}\log p,$$

where C is a constant depending only on d.

In the present note, in particular, this conjecture is confirmed as a special case of a general result on the least residue of a finite system of polynomials, and the estimate is improved by a factor $\log p$.

For simplicity we shall restrict ourselves to a system of two polynomials and shall henceforth use the following notation: $F(X), G(Y)$ are polynomials of degrees d, δ with integer coefficients, considered over the field $[p]$, where p is a growing prime number; $\Phi(X,Y) = (F(X) - F(Y))/(X - Y)$; $r(m), \rho(m)$ are the numbers of solutions of the congruences $F(X) \equiv m(\mathrm{mod}p)$ and $G(Y) \equiv m(\mathrm{mod}p)$, respectively $(1 \leq m \leq p)$; ν is the least common natural residue of the polynomials $F(X), G(Y)$ modulo p; μ is the least natural number which is simultaneously a nonresidue of $F(X)$ and a residue of $G(Y)$. Throughout, unless explicitly stated otherwise, it is assumed that the constant in the symbol O depends only on d, δ.

Theorem 1. *If the polynomial $F(X) - G(Y)$ has at least one divisor absolutely irreducible over $[p]$, and $1 \leq d, \delta < p$, then there exists a constant C, depending only on d, δ, such that for all sufficiently large p the number ν exists and*

$$1 \leq \nu < C\sqrt{p}.$$

Remark. The condition of the theorem will certainly be fulfilled for all sufficiently large p if one assumes that $F(X) - G(Y)$ has at least one divisor absolutely irreducible over the field of rational numbers.

Corollary. For all polynomials of degree d $(1 \le d < p)$, the pair $(m, m+1)$ of least consecutive residues has the estimate

$$m = O(\sqrt{p}).$$

This is obtained by taking $G(Y) = F(Y) - 1$, since the polynomial $F(X) - F(Y) + 1$ is absolutely irreducible.

Theorem 2. *Suppose that the following conditions are satisfied:*

1) $2 \le d < p, \quad 1 \le \delta < p.$
2) *The polynomial* $F(X) - G(Y)$ *has exactly one divisor absolutely irreducible over* $[p]$.
3) *The curve* $\Phi(X, Y) = 0$, $F(X) - G(Z) = 0$ *has at least one absolutely irreducible component defined over* $[p]$.

Then there exists a constant C, *depending only on* d, δ, *such that for all sufficiently large* p *the number* μ *exists and*

$$1 \le \mu < C\sqrt{p}.$$

Let us note that, in a certain sense, the conditions of Theorems 1 and 2 are necessary. For example, if one sets $F(X) = X^2$, $G(Y) = 2Y^2$, then for all p satisfying $(2/p) = -1$ the polynomial $X^2 - 2Y^2$ will be irreducible over $[p]$, but not absolutely irreducible, and, obviously, the number v does not exist. If, further, one sets $F(X) = X^2$, $G(Y) = Y^2$, then all the conditions of Theorem 2 will be satisfied except condition 2), and the number μ does not exist.

Theorem 2 with $G(Y) = Y$ turns into the known result of Bombieri and Davenport ([2]), improved in ([3]).

The proofs are based on the following lemmas.

Lemma 1. Let u be an integer satisfying $1 \le u \le (p-1)/2$; let $k(m)$ be the number of solutions of the congruence $x + y \equiv m \pmod p$, where $1 \le x \le u$, $1 \le y \le u$. Then for every complex-valued function $\lambda(m)$ we have:

$$\sum_{m=1}^{p} \lambda(m) k(m) = \frac{u^2}{p} \sum_{m=1}^{p} \lambda(m) + O(uR),$$

where the constant in the symbol O is absolute and

$$R = \max_{1 \le t \le p-1} \left| \sum_{m=1}^{p} \lambda(m) \exp\left(\frac{2\pi i}{p} tm\right) \right|.$$

Proof with insignificant changes in notation is contained in ([3]).

Lemma 2. If the polynomial $F(X) - G(Y)$ has e distinct factors, absolutely irreducible over $[p]$, and $1 \leq d,\ \delta < p$, then

$$\sum_{m=1}^{p} r(m)\rho(m)k(m) = eu^2 + O(u\sqrt{p}).$$

Proof. Apply Lemma 1 with $\lambda(m) = r(m)\rho(m)$. The sum

$$\sum_{m=1}^{p} r(m)\rho(m)$$

is equal to the number of points of the curve $F(X) - G(Y) = 0$ having coordinates in $[p]$. Each component defined over $[p]$ gives $p + O(\sqrt{p})$ points by the known results of ([4]). The number of points common to two or more components, and also the number of points corresponding to components defined over a proper extension of the field $[p]$, has estimate $O(1)$ (see, for example, ([5])). Consequently,

$$\sum_{m=1}^{p} r(m)\rho(m) = ep + O(\sqrt{p}).$$

Further, for $1 \leq t \leq p-1$,

$$\sum_{m=1}^{p} r(m)\rho(m) \exp\left(\frac{2\pi i}{p}\, tm\right) = \sum \exp\left(\frac{2\pi i}{p}\, tF(x)\right),$$

where the summation is carried out along the curve $F(X) - G(Y) = 0$. By the results of ([5]) on exponential sums along a curve (see also ([2])) this sum is $O(\sqrt{p})$. The assertion now follows from Lemma 1.

Lemma 3. Let the following conditions be satisfied:

1) $2 \leq d < p, \quad 1 \leq \delta < p$.
2) The polynomial $F(X) - G(Y)$ has e distinct factors, absolutely irreducible over $[p]$.
3) The curve $\Phi(X, Y) = 0,\ F(X) - G(Z) = 0$ has e' distinct components, absolutely irreducible over $[p]$.

Then

$$\sum_{m=1}^{p} r^2(m)\rho(m)k(m) = (e + e')u^2 + O(u\sqrt{p}).$$

Proof. Setting $\lambda(m) = r^2(m)\rho(m)$ and arguing in the same way as above, we arrive at summation along the curve $F(X) - F(Y) =$

$= 0, F(X) - G(Z) = 0$, which is representable as a union of the curves $X - Y = 0, F(X) - G(Z) = 0, \Phi(X, Y) = 0, F(X) - G(Z) = 0$. These curves give, respectively, $e(p + O(\sqrt{p}))$ and $e'(p + O(\sqrt{p}))$ points. The remainder term R is estimated in the same way as in Lemma 2.

Lemma 4. If $1 \leq \delta < p$, then

$$\sum_{m=1}^{p} \rho(m)k(m) = u^2 + O(u\sqrt{p}).$$

This follows from Lemma 2 for $F(X) = X$.

Proof of Theorem 1. Setting in Lemma 2 $u = C_1\sqrt{p}$, where C_1 is a suitably chosen constant, and taking into account that $e \geq 1$ and $k(m) = 0$ when $m > 2u$, we obtain

$$\sum_{m=1}^{2u} r(m)\rho(m)k(m) > 0$$

and, consequently, ν exists and has the estimate $\nu = O(\sqrt{p})$.

Proof of Theorem 2. Setting

$$N_h = \sum_{r(m)=h} \rho(m)k(m)$$

$(0 \leq h \leq d)$ and applying Lemma 4 and Lemmas 2, 3 for $e = 1$, $e' \geq 1$, we obtain (see (2))

$$N_0 = \sum_{\substack{r(m)=0 \\ 1 \leq m \leq 2u}} \rho(m)k(m) > 0,$$

where $u = O(\sqrt{p})$.

It would be interesting to obtain an analogous result for the general least non-residue of polynomials F and G; however, the method presented here in this case requires refinement.

The estimates of exponential sums used here can be generalized to sums of a more general form

$$\sum_{P} e(\varphi(P))\chi(\psi(P)),$$

where e, χ are additive and multiplicative characters of the finite field k; φ, ψ are functions on an algebraic curve defined over k, and the summation is over the points P of the curve rational over k. Using such estimates, one can refine the result of Theorems 1 and 2 in the case when $G(Y) = Y^k$, where $k \mid p - 1$. The following can be proved.

Theorem 3. Let the integer $k \mid p-1$; let $F(X)$ be a polynomial of degree d, where $2 \leq d < p$. Suppose that the following conditions are satisfied:

1) The polynomial $\Phi(X, Y)$ has at least one factor absolutely irreducible over $[p]$.

2) $F(X) \neq af^l(X)$, where $a \in [p]$, $f(X)$ is a polynomial over $[p]$, $l \mid k,\ l > 1$.

Then there exists a constant C, depending only on d, and k-th power residues $\lambda, \mu \pmod p$, satisfying the conditions:

1) $1 \leq \lambda,\ \mu < Ck\sqrt{p}$.

2) The congruence $F(X) \equiv \lambda \pmod p$ is solvable.

3) The congruence $F(X) \equiv \mu \pmod p$ is not solvable.

Note added in proof. K. Williams proved his conjecture in paper (6), which became known to the author only after the present article had been submitted for publication. However, K. Williams' s result is obtained as a very special consequence of our results.

Saratov State University
named after N. G. Chernyshevsky

Received
25 IV 1968

REFERENCES

1. K. S. Williams, Canad. J. Math., 19, No. 3, 655 (1967).
2. E. Bombieri, H. Davenport, Am. J. Math., 88, No. 1, 61 (1966).
3. A. Tietäväinen, Turun Yliopiston Julk, Sar A, I, No. 94, 6 (1966).
4. S. Lang, A. Weil, Am. J. Math., 76, No. 1–4, 819 (1954).
5. E. Bombieri, Am. J. Math., 88, No. 1, 71 (1966).
6. K. S. Williams, Canad. Math. Bull., 11, No. 1, 79 (1968).

Note: Figure translations are in progress. See original paper for figures.