NOTE ON PAIRS OF CONSECUTIVE RESIDUES OF POLYNOMIALS

Kenneth S. Williams

(received August 4, 1967)

1. Introduction. Let $f(x)$ be a polynomial of degree $d \geq 3$ with integral coefficients, say,

$$f(x) = a_o + a_1 x + \dots + a_d x^d . \tag{1}$$

In a previous paper [6] I deduced, from a deep result of Lang and Weil [2], that there is a constant $k_1(d)$, depending only on d, such that for all primes $p \geq k_1(d)$, $p \nmid a_d$, $f(x)$ has a pair of consecutive residues (mod p), that is, there exists an integer $r (0 \leq r \leq p-1)$ with the property that

$$f(x) \equiv r, \quad f(y) \equiv r + 1 \pmod p \tag{2}$$

are simultaneously soluble. It was further proved that for almost all polynomials of degree d, the least such r (say e) satisfies

$$e \leq k_2(d) p^{\frac{1}{2}} \log p \qquad (p \geq k_1(d)) \tag{3}$$

for some constant $k_2(d)$ depending only on d. I conjectured that, in fact, (3) holds for all such polynomials. K. McCann and I have proved this when $d = 3$ (see [3]) and when $d = 4$ (see [4]). It is the purpose of this note to prove the conjecture in the stronger form:

THEOREM. There is a constant $k_3(d)$, depending only on d, such that for all primes $p \geq k_1(d)$,

$$e \leq k_3(d) p^{\frac{1}{2}} . \tag{4}$$

To prove this theorem, we use a recent deep result of Bombieri and Davenport [1] and a method of Tietäväinen [5].

2. Proof of theorem. Let h be an integer such that $1 \le h \le \frac{1}{2}(p+1)$, so that $0 \le h-1 \le \frac{1}{2}(p-1)$. Set $H = \{0, 1, 2, \ldots, h-1\}$ and write $H_r\ (r = 0, 1, 2, \ldots, p-1)$ for the number of solutions of

$$(5) \qquad x + y \equiv r \qquad (\mathrm{mod}\ p) \qquad x \in H,\ y \in H$$

so that

$$(6) \qquad pH_r = \sum_{t=0}^{p-1} \sum_{x=0}^{h-1} \sum_{y=0}^{h-1} e\{t(x+y-r)\}$$

where $e(u) = \exp(2\pi i u/p)$. Now let $N_r\ (r = 0, 1, 2, \ldots, p-1)$ denote the number of solutions of $f(x) \equiv r\ (\mathrm{mod}\ p)$. Then

$$(7) \qquad p \sum_{r=0}^{p-1} N_r N_{r+1} H_r = \sum_{t=0}^{p-1} S(t) \left\{ \sum_{x=0}^{h-1} e(tx) \right\}^2$$

where

$$(8) \qquad S(t) = \sum_{r=0}^{p-1} N_r N_{r+1}\, e(-tr) .$$

I proved in [6] that

$$S(t) = \sum_{\substack{x,\, y=0 \\ f(y)-f(x)-1 \equiv 0}}^{p-1} e(tf(x))$$

and also that $f(y) - f(x) - 1$ is absolutely irreducible $(\mathrm{mod}\ p)$. Hence for $t \ne 0$, a result of Bombieri and Davenport [1] implies that

$$(9) \qquad |S(t)| \le k_4(d) p^{\frac{1}{2}} \qquad (p \ge k_1(d)),$$

where $k_4(d)$ is a constant depending only on d. For $t = 0$

a result of Lang and Weil [2] gives

$$(10)\qquad |S(0) - p| \le k_5(d)p^{\frac{1}{2}} \qquad (p \ge k_1(d)),$$

where $k_5(d)$ is a constant depending only on d. Thus

$$\left| p \sum_{r=0}^{p-1} N_r N_{r+1} H_r - h^2 S(0) \right|$$

$$= \left| \sum_{t=1}^{p-1} S(t) \{ \sum_{x=0}^{h-1} e(tx) \}^2 \right|$$

$$\le \sum_{t=1}^{p-1} |S(t)| \left| \sum_{x=0}^{h-1} e(tx) \right|^2$$

$$\le k_4(d)p^{\frac{1}{2}} \sum_{t=1}^{p-1} \left| \sum_{x=0}^{h-1} e(tx) \right|^2 ,$$

by (9). In [5] it was noted that

$$\sum_{t=1}^{p-1} \left| \sum_{x=1}^{h-1} e(tx) \right|^2 = h(p-h)$$

so using (10) we have

$$p \sum_{r=0}^{p-1} N_r N_{r+1} H_r \ge h^2 S(0) - k_4(d)p^{\frac{1}{2}} h(p-h)$$

$$\ge h^2(p - k_5(d)p^{\frac{1}{2}}) - k_4(d)hp^{3/2}$$

$$\ge h^2 p - (k_4(d)+k_5(d))hp^{3/2}$$

$$= ph\{h - (k_4(d)+k_5(d))p^{\frac{1}{2}}\}.$$

Choose $h = [\{k_4(d)+k_5(d)\} p^{\frac{1}{2}}] + 1$ so that

$$\sum_{r=0}^{p-1} N_r N_{r+1} H_r > 0 .$$

Hence there exists r $(0 \leq r \leq p-1)$ for which

$$N_r > 0, \; N_{r+1} > 0, \; H_r > 0;$$

i.e., for which $(r, r+1)$ is a pair of consecutive residues of $f(x)$ and moreover

$$r = x+y \qquad\qquad x \varepsilon H, \; y \varepsilon H$$

so that

$$0 \leq r \leq 2(h-1) = 2[\{k_4(d)+k_5(d)\} p^{\frac{1}{2}}] \quad .$$

Hence

$$e \leq k_3(d)p^{\frac{1}{2}}$$

where

$$k_3(d) = 2\{k_4(d)+k_5(d)\} .$$

which proves (4).

REFERENCES

1. E. Bombieri and H. Davenport, On two problems of Mordell, Amer. J. Math., 88 (1966), 61-70.

2. S. Lang and A. Weil, Number of points of varieties in finite fields, Amer. J. Math., 76 (1954), 819-827.

3. K. McCann and K. S. Williams, On the residues of a cubic polynomial (mod p), Canad. Math. Bull., 10 (1967), 29-38.

4. K. McCann and K. S. Williams, The distribution of the residues of a quartic polynomial, Glasgow Math. Journal 8 (1967), 67-88.

5. A. Tietäväinen, On non-residues of a polynomial, Ann. Univ. Turku., Ser. Al, 94 (1966), 3-6.

6. K.S. Williams, Pairs of consecutive residues of polynomials, Can. J. Math., 19 (1967), 655-666.

Carleton University