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,

\[
f(x) = a_0 + a_1 x + \ldots + a_d x^d.
\]

In a previous paper [6] I deduced, from a deep result of Lang and Weil [2], that there is a constant \( k_4(d) \), depending only on \( d \), such that for all primes \( p \geq k_4(d) \), \( p \nmid a_d \), \( f(x) \) has a pair of consecutive residues \( \pmod{p} \), that is, there exists an integer \( r \) \((0 < r < p-1)\) with the property that

\[
f(x) \equiv r \pmod{p}, \quad f(y) \equiv r + 1 \pmod{p}
\]

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

\[
e \leq k_2(d)p^{\frac{1}{2}} \log p \quad (p \geq k_4(d))
\]

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 \( p \geq k_4(d) \),

\[
e \leq k_3(d)p^{\frac{1}{2}}.
\]
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 $1 \leq h \leq \frac{1}{2} (p+1)$, so that $0 < h-1 < \frac{1}{2} (p-1)$. 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

$$x + y \equiv r \pmod{p} \quad x, y \in H$$

so that

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

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 $f(x) \equiv r \pmod{p}$. Then

$$P = \sum_{r=0}^{p-1} N_r \cdot N_{r+1} = \sum_{t=0}^{p-1} S(t) \sum_{x=0}^{p-1} e(-tr)$$

where

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

I proved in [6] that

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

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

$$\left| S(t) \right| \leq k_4(d)p^2 \quad (p \geq k_4(d)),$$

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

80
a result of Lang and Weil [2] gives

\[ |S(0) - p| \leq \frac{k_5(d)}{2} p^2 \quad (p \geq k_4(d)), \]

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

\[
\begin{align*}
|p \sum_{r=0}^{p-1} \frac{1}{N_r N_{r+1} H_r} - h^2 S(0)| &= \left| \sum_{t=1}^{p-1} S(t) \left\{ \sum_{x=0}^{h-1} e(tx) \right\}^2 \right| \\
&\leq \sum_{t=1}^{p-1} |S(t)| \sum_{x=0}^{h-1} |e(tx)|^2 \\
&\leq k_4(d)p^2 \sum_{t=1}^{p-1} |S(t)| \sum_{x=0}^{h-1} |e(tx)|^2,
\end{align*}
\]

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

\[
\sum_{t=1}^{p-1} \sum_{x=0}^{h-1} |e(tx)|^2 = h(p-h)
\]

so using (10) we have

\[
\begin{align*}
p \sum_{r=0}^{p-1} \frac{1}{N_r N_{r+1} H_r} &\geq h^2 S(0) - k_4(d)p^2 \frac{1}{2} h(p-h) \\
&\geq h^2 (p - k_5(d)p^{1/2}) - k_4(d)h^{3/2} \\
&\geq h^2 p - (k_4(d)+k_5(d))h^{3/2} \\
&= ph \left\{ h - (k_4(d)+k_5(d))p^2 \right\}.
\end{align*}
\]
Choose \( h = \left[ \{k_4(d)+k_5(d)\} \frac{1}{p^2} \right] + 1 \) so that
\[
\sum_{r=0}^{p-1} N_r N_{r+1} H > 0.
\]

Hence there exists \( r \) \((0 \leq r \leq p-1)\) for which
\[
N_r > 0, \quad N_{r+1} > 0, \quad H_r > 0;
\]
i.e., for which \((r, r+1)\) is a pair of consecutive residues of \( f(x) \) and moreover
\[
r = x+y \quad \quad \quad x \in H, \ y \in H
\]
so that
\[
0 \leq r \leq 2(h-1) = 2\left[\left\{k_4(d)+k_5(d)\right\} \frac{1}{p^2}\right].
\]

Hence
\[
e \leq k_3(d)p^2
\]
where
\[
k_3(d) = 2\{k_4(d)+k_5(d)\}.
\]

which proves (4).

REFERENCES


Carleton University