PAIRS OF CONSECUTIVE RESIDUES OF POLYNOMIALS

KENNETH S. WILLIAMS

1. Introduction. Let p be a large prime and let $f(x)$ be a polynomial of fixed degree $d \geqslant 4$ with integral coefficients, say,

$$f(x) = a_0 + a_1 x + \ldots + a_d x^d \qquad (a_d \not\equiv 0 \pmod{p}). \tag{1.1}$$

Recently Mordell **(8)** has considered the problem of estimating the least positive residue of $f(x) \pmod{p}$, that is, the unique integer l $(0 \leqslant l \leqslant p-1)$ such that the congruence

$$f(x) \equiv r \pmod{p} \tag{1.2}$$

is soluble for $r = l$ but not for $r = 0, 1, \ldots, l-1$.

Let N_r $(r = 0, 1, \ldots, p-1)$ denote the number of solutions of (1.2). Then

$$\sum_{r=0}^{p-1} N_r = p. \tag{1.3}$$

This proves that l always exists and Mordell establishes that

$$l \leqslant dp^{\frac{1}{2}} \log p. \tag{1.4}$$

If we let $e(u)$ denote $\exp(2\pi\, iup^{-1})$, for any real number u, we have

$$N_r = \frac{1}{p}\sum_{x,\,t=0}^{p-1} e(t(f(x) - r)), \tag{1.5}$$

since as the sum in t is zero if $f(x) \not\equiv r$ and is p if $f(x) \equiv r \pmod{p}$. (We usually omit "mod p" hereafter.) Mordell's proof of (1.4) consists of using (1.5) and a deep result of Carlitz and Uchiyama **(3)** to show that

$$lp = \left| p\sum_{r=0}^{l-1} N_r - lp \right| \leqslant dp\sqrt{p}\log p. \tag{1.6}$$

The deep result quoted, which is a consequence of Weil's proof of the Riemann hypothesis for algebraic function fields over a finite field **(10)**, is the following:

$$\left| \sum_{x=0}^{p-1} e(f(x)) \right| \leqslant d\sqrt{p}. \tag{1.7}$$

The purpose of this paper is to consider the similar problem for pairs of consecutive residues of $f(x)$, that is we require an estimate for the least

Received May 11, 1966.

integer e $(0 \leqslant e \leqslant p-1)$ with the property that both e and $e+1$ are residues of $f(x)$, i.e. the pair of congruences

$$(1.8) \qquad f(x) \equiv r, \qquad f(y) \equiv r+1$$

are soluble for $r = e$ but not for $r = 0, 1, \ldots, e-1$.

The number of incongruent solutions (x, y) of (1.8) is, of course, $N_r N_{r+1}$ and it is easy to see that

$$(1.9) \qquad \sum_{r=0}^{p-1} N_r N_{r+1} = N_f,$$

where N_f denotes the number of solutions (x, y) of the congruence

$$(1.10) \qquad f(y) - f(x) - 1 \equiv 0.$$

If $N_f = 0$, then each summand in (1.9) (being non-negative) is zero and e does not exist. It is clear then that a necessary and sufficient condition for the existence of e is that $N_f > 0$. In Theorem 1 we show, using a deep result of Lang and Weil **(6)**, that

$$(1.11) \qquad N_f = p + O(p^{\frac{1}{2}}),$$

where the constant implied by the O-symbol depends only on d. This implies that

$$(1.12) \qquad N_f \geqslant c_d\, p,$$

where c_d is a constant depending only on d, for sufficiently large primes p and so e always exists for large enough p. However, when p is small, e may not exist, for consider $f(x) = 2x^4$ when $p = 5$. In this case the residues are 0 and 2 and so there are no consecutive ones.

Our method for estimating e for large p follows that of Mordell for l. Instead of considering

$$\sum_{r=0}^{l-1} N_r$$

(as in (1.6)) we consider

$$(1.13) \qquad \sum_{r=0}^{e-1} N_r N_{r+1}.$$

After replacing N_r and N_{r+1} by exponential sums (see § 5) we find that we need to consider the sums

$$(1.14) \qquad S(v) = \sum_{r=0}^{p-1} N_r N_{r+1}\, e(-rv) \qquad (v = 1, 2, \ldots, p-1).$$

We, in fact, need an upper bound for $|S(v)|$, which is independent of v. From (1.14) it is easy to see that we require a suitable estimate for an exponential sum of the type

$$(1.15) \qquad \sum_{\substack{x,y=0 \\ h(x,y)\equiv 0}}^{p-1} e(g(x, y)),$$

where g and h are polynomials in the two variables x and y. (In our case $g(x, y) = vf(x)$ and $h(x, y) = f(y) - f(x) - 1$.) It seems very difficult to estimate such a sum effectively. In fact our knowledge of the similar sum

$$(1.16) \qquad \sum_{x,y=0}^{p-1} e(g(x, y))$$

is slight, except in a few special cases (5). We are thus forced to estimate $|S(v)|$ for almost all polynomials of fixed degree d. This involves determining an upper bound for

$$(1.17) \qquad S = \sum_{\substack{f \\ \deg f=d}} |S(v)|^2,$$

which is independent of v. (Without loss of generality, the summation over f involves summing a_i from 0 to $p - 1$ ($i = 1, 2, \ldots, d - 1$) and a_d from 1 to $p - 1$.) This is done in Theorem 2. Our final result is

THEOREM 3. *For almost all polynomials of fixed degree d, we have*

$$e = O(p^{\frac{1}{2}} \log p),$$

where the constant implied by the O-symbol depends only on d.

2. Proof of Theorem 1. In this section we regard the coefficients of f as reduced modulo p and considered as belonging to $[p]$, the Galois field with p elements.

THEOREM 1. $N_f = p + O(p^{\frac{1}{2}})$, *where the constant implied by the O-symbol depends only on d.*

Proof. Let

$$(2.1) \qquad g(x, y, z) = z^d + z^d(f(x/z) - f(y/z)) = z^d + g_1 z^{d-1} + \ldots + g_d,$$

where

$$(2.2) \qquad g_i \equiv g_i(x, y) = a_i(x^i - y^i) \qquad (i = 1, 2, \ldots, d).$$

As $x - y \mid g_i$ for $i = 1, 2, \ldots, d$ and $(x - y)^2 \nmid g_d$ over $[p]$, by Eisenstein's irreducibility criterion, $g(x, y, z)$ is irreducible over $[p]$. Suppose, however, that g is not absolutely irreducible over $[p]$; then there is a normal extension $N[p]$ of $[p]$ over which g splits into $c \geqslant 2$ conjugate factors, say

$$(2.3) \qquad g(x, y, z) = \prod_{i=1}^{c} f_i(x, y, z).$$

Let

$$(2.4) \qquad k_i(x, y) = f_i(x, y, 0) \qquad (i = 1, 2, \ldots, c);$$

then

$$(2.5) \qquad \prod_{i=1}^{c} k_i(x, y) = a_d(x^d - y^d).$$

https://doi.org/10.4153/CJM-1967-060-1 Published online by Cambridge University Press

Hence $x - y \mid k_i(x, y)$ over $N[p]$ for some i, and so by conjugacy for all i. Let

(2.6) $$k_i(x, y) = (x - y)h_i(x, y);$$

then

(2.7) $$a_d(x^d - y^d) = (x - y)^c h(x, y),$$

where

$$h(x, y) = \prod_{i=1}^{c} h_i(x, y)$$

has coefficients in $[p]$. This is a contradiction since $c \geqslant 2$, and so $g(x, y, z)$ is absolutely irreducible over $[p]$. Hence by a result of Lang and Weil **(6)** the number of solutions (x, y, z) of

(2.8) $$g(x, y, z) = 0 \pmod p)$$

is

(2.9) $$p^2 + O(p^{3/2}),$$

where the constant implied by the O-symbol depends only on d. Now the number of solutions (x, y) of

(2.10) $$g(x, y, 0) \equiv 0 \pmod p),$$

that is of

(2.11) $$x^d - y^d \equiv 0,$$

is certainly $O(p)$, so the number of solutions (x, y, z) with $z = 0$ of (2.8) is also given by

(2.12) $$p^2 + O(p^{3/2}).$$

Hence the number of solutions (x, y) of

(2.13) $$g(x, y, 1) \equiv 0,$$

that is, of

(2.14) $$f(y) - f(x) - 1 \equiv 0,$$

is just

(2.15) $$\frac{1}{p-1}\{p + O(p^{3/2})\} = p + O(p^{1/2}),$$

as required.

3. Some useful lemmas.

Definition. Let $N_d \equiv N_d\ (a_1, \ldots, a_k)$ denote the number of solutions $(x_1, \ldots, x_k)$ of the system of d congruences

$$(3.1)\qquad \begin{array}{l} a_1 x_1 + \ldots + a_k x_k \equiv 0, \\ a_1 x_1^2 + \ldots + a_k x_k^2 \equiv 0, \quad (\text{mod } p). \\ \cdot \quad \cdot \quad \cdot \\ a_1 x_1^d + \ldots + a_k x_k^d \equiv 0. \end{array}$$

We require the following lemmas for the proof of Theorem 2. They give asymptotic formulae for $N_d\ (a_1, \ldots, a_k)$, when $k = 2,\ d \geqslant 2;\ k = 3,\ d \geqslant 3$; and $k = 4,\ d \geqslant 4$.

LEMMA 3.1. *If $a_1, a_2 \not\equiv 0$ and $d \geqslant 2$,*

$$(3.2)\qquad N_d(a_1, a_2) = \begin{cases} 1, & \text{if } a_1 + a_2 \not\equiv 0, \\ p, & \text{if } a_1 + a_2 \equiv 0. \end{cases}$$

Proof. The result is obvious, since the only solution when $a_1 + a_2 \not\equiv 0$ is $(x_1, x_2) = (0, 0)$ and the only solutions when $a_1 + a_2 \equiv 0$ are given by $(x_1, x_2) = (x, x)$ $(x = 0, 1, \ldots, p - 1)$.

LEMMA 3.2. *If $a_1, a_2, a_3 \not\equiv 0$ and $d \geqslant 3$,*

$$(3.3)\qquad N_d(a_1, a_2, a_3) = \begin{cases} O(1), & \text{if } a_1 + a_2, a_2 + a_3, a_3 + a_1, a_1 + a_2 + a_3 \not\equiv 0, \\ p + O(1), & \text{if } a_1 + a_2 + a_3 \equiv 0 \text{ or } a_1 + a_2 + a_3 \not\equiv 0, \\ & \quad \text{and exactly one of } a_1 + a_2,\ a_2 + a_3,\ a_3 + a_1 \equiv 0, \\ 2p + O(1), & \text{if } a_1 + a_2 + a_3 \not\equiv 0 \text{ and exactly two of} \\ & \quad a_1 + a_2,\ a_2 + a_3,\ a_3 + a_1 \equiv 0. \end{cases}$$

Proof. Let $N_d^*\ (a_1, a_2, a_3)$ be the number of solutions of (3.1) $(d \geqslant 3,\ k = 3)$ with $x_i \not\equiv x_j$ $(1 \leqslant i < j \leqslant 3)$. Since $d \geqslant 3$, for these solutions,

$$(3.4)\qquad \text{rank} \begin{bmatrix} a_1 & a_2 & a_3 \\ 2a_1 x_1 & 2a_2 x_2 & 2a_3 x_3 \\ \cdot & \cdot & \cdot \\ da_1 x_1^{d-1} & da_2 x_2^{d-1} & da_3 x_3^{d-1} \end{bmatrix} = 3,$$

and so by a result of Min (**7**, Theorem 1)

$$(3.5)\qquad N_d^*(a_1, a_2, a_3) = O(1),$$

where the constant implied by the O-symbol depends only on d. Let $N_d^{(ij)}$ (a_1, a_2, a_3) $(1 \leqslant i < j \leqslant 3)$ denote the number of solutions of (3.1) $(d \geqslant 3,\ k = 3)$ with $x_i \equiv x_j$. Also let $N_d^{(123)}(a_1, a_2, a_3)$ denote the number with $x_1 \equiv x_2 \equiv x_3$. Then

$$(3.6)\qquad N_d(a_1, a_2, a_3) = N_d^*(a_1, a_2, a_3) + \{N_d^{(12)}(a_1, a_2, a_3) + N_d^{(13)}(a_1, a_2, a_3) + N_d^{(23)}(a_1, a_2, a_3)\} - 2N_d^{(123)}(a_1, a_2, a_3),$$

and so by (3.5) we have

$$(3.7)\qquad N_d(a_1, a_2, a_3) = \{N_d(a_1 + a_2, a_3) + N_d(a_2 + a_3, a_1) + N_d(a_3 + a_1, a_2)\} - 2N_d^{(123)}(a_1, a_2, a_3) + O(1).$$

The result then follows from Lemma 3.1 and the obvious result

$$(3.8) \qquad N_d^{(123)}(a_1, a_2, a_3) = \begin{cases} p, & \text{if } a_1 + a_2 + a_3 \equiv 0, \\ 1, & \text{if } a_1 + a_2 + a_3 \not\equiv 0. \end{cases}$$

LEMMA 3.3. *If* $a_1, a_2, a_3, a_4 \not\equiv 0$ *and* $d \geqslant 4$, $N_d(a_1, a_2, a_3, a_4)$ *is given by the expression* (3.12), *the terms of which are given by Lemmas* 3.1 *and* 3.2 *and* (3.13).

Proof. Let $N_d^*(a_1, a_2, a_3, a_4)$ denote the number of solutions of (3.1) ($d \geqslant 4$, $k = 4$) with $x_i \not\equiv x_j$ $(1 \leqslant i < j \leqslant 4)$. For these solutions

$$(3.9) \qquad \text{rank} \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ 2a_1 x_1 & 2a_2 x_2 & 2a_3 x_3 & 2a_4 x_4 \\ \cdot & \cdot & \cdot & \cdot \\ da_1 x_1^{d-1} & da_2 x_2^{d-1} & da_3 x_3^{d-1} & da_4 x_4^{d-1} \end{bmatrix} = 4$$

and so, using Min's theorem again, we have

$$(3.10) \qquad N_d^*(a_1, a_2, a_3, a_4) = O(1),$$

where the constant implied by the O-symbol depends only on d. Let $N_d^{(ij)}$ (a_1, a_2, a_3, a_4) $(1 \leqslant i < j \leqslant 4)$ denote the number of solutions of (3.1) ($d \geqslant 4$, $k = 4$) with $x_i \equiv x_j$ and $N_d^{(ijk)}(a_1, a_2, a_3, a_4)$ $(1 \leqslant i < j < k \leqslant 4)$ the number with $x_i \equiv x_j \equiv x_k$. Finally let $N_d^{(1234)}(a_1, a_2, a_3, a_4)$ denote the number with $x_1 \equiv x_2 \equiv x_3 \equiv x_4$. Then

$$(3.11) \qquad N_d(a_1, a_2, a_3, a_4) = N_d^*(a_1, a_2, a_3, a_4) + \sum_{1 \leqslant i < j \leqslant 4} N_d^{(ij)}(a_1, a_2, a_3, a_4)$$
$$- \sum_{\substack{1 < i \leqslant 4 \\ 1 < j < k \leqslant 4 \\ j, k \neq i}} N_d^{(ijk)}(a_1, a_2, a_3, a_4) - 2 \sum_{1 \leqslant i < j < k \leqslant 4} N_d^{(ijk)}(a_1, a_2, a_3, a_4)$$
$$+ 6N_d^{(1234)}(a_1, a_2, a_3, a_4),$$

and so

$$(3.12) \qquad N_d(a_1, a_2, a_3, a_4) = \{N_d(a_1 + a_2, a_3, a_4) + N_d(a_1 + a_3, a_2, a_4)$$
$$+ N_d(a_1 + a_4, a_2, a_3) + N_d(a_2 + a_3, a_1, a_4) + N_d(a_2 + a_4, a_1, a_3)$$
$$+ N_d(a_3 + a_4, a_1, a_2)\} - \{N_d(a_1 + a_2, a_3 + a_4) + N_d(a_1 + a_3, a_2 + a_4)$$
$$+ N_d(a_1 + a_4, a_2 + a_3)\} - 2\{N_d(a_1 + a_2 + a_3, a_4) + N_d(a_1 + a_2 + a_4, a_3)$$
$$+ N_d(a_1 + a_3 + a_4, a_2) + N_d(a_2 + a_3 + a_4, a_1)\} + 6N_d^{(1234)}(a_1, a_2, a_3, a_4)$$
$$+ O(1).$$

It is clear that

$$(3.13) \qquad N_d^{(1234)}(a_1, a_2, a_3, a_4) = \begin{cases} p, & \text{if } a_1 + a_2 + a_3 + a_4 \equiv 0, \\ 1, & \text{if } a_1 + a_2 + a_3 + a_4 \not\equiv 0, \end{cases}$$

and that the rest of the terms in (3.12) can be evaluated by Lemmas 3.1 and 3.2.

4. Proof of Theorem 2. We prove

THEOREM 2. *For almost all polynomials of fixed degree d, there is a constant k_d (depending only on d) such that*

$$\max_{1\leqslant v\leqslant p-1} |S(v)| \leqslant k_d p^{\frac{1}{2}}. \tag{4.1}$$

Proof. We have, on adding in the term corresponding to $a_d = 0$,

$$S = \sum_{\substack{f \\ \deg f=d}} |S(v)|^2 \leqslant \sum_{a_0, a_1, \ldots, a_d=0}^{p-1} |S(v)|^2. \tag{4.2}$$

Now

$$|S(v)|^2 = \left| \sum_{b=0}^{p-1} N_b N_{b+1} e(-bv) \right|^2 \tag{4.3}$$

$$= \sum_{b,c=0}^{p-1} N_b N_{b+1} N_c N_{c+1} e((c-b)v)$$

and because

$$N_b N_{b+1} N_c N_{c+1} = \left\{\frac{1}{p}\sum_{x_1,t_1=0}^{p-1} e(t_1(f(x_1)-b))\right\}\left\{\frac{1}{p}\sum_{x_2,t_2=0}^{p-1} e(t_2(f(x_2)-b-1))\right\}$$

$$\times \left\{\frac{1}{p}\sum_{x_3,t_3=0}^{p-1} e(t_3(f(x_3)-c))\right\}\left\{\frac{1}{p}\sum_{x_4,t_4=0}^{p-1} e(t_4(f(x_4)-c-1))\right\}$$

$$= \frac{1}{p^4} \sum_{\substack{x_1,x_2,x_3,x_4, \\ t_1,t_2,t_3,t_4=0}}^{p-1} e(-bt_1 - (b+1)t_2 - ct_3 - (c+1)t_4)$$

$$\times e(t_1 f(x_1) + t_2 f(x_2) + t_3 f(x_3) + t_4 f(x_4))$$

$$= \frac{1}{p^4} \sum_{x_1,\ldots,t_4=0}^{p-1} e(-bt_1 - (b+1)t_2 - ct_3 - (c+1)t_4)$$

$$\times \left\{ \prod_{i=0}^{d} e(a_i(t_1 x_1^i + t_2 x_2^i + t_3 x_3^i + t_4 x_4^i)) \right\},$$

we have

$$p^4 S \leqslant \sum_{t_1,t_2,t_3,t_4=0}^{p-1} e(-(t_2+t_4)) \sum_{x_1,x_2,x_3,x_4=0}^{p-1} \left\{ \prod_{i=0}^{d} \sum_{a_i=0}^{p-1} e(a_i(t_1 x_1^i + \ldots + t_4 x_4^i)) \right\}$$

$$\times \sum_{b=0}^{p-1} e(-(v+t_1+t_2)b) \sum_{c=0}^{p-1} e((v-t_3-t_4)c)$$

and so

$$p^2 S \leqslant \sum_{t_1,t_3=0}^{p-1} e(t_1+t_3) \sum_{x_1,x_2,x_3,x_4=0}^{p-1} \left\{ \prod_{i=0}^{d} \sum_{a_i=0}^{p-1} e(a_i(t_1 x_1^i - (t_1+v)x_2^i + t_3 x_3^i - (t_3-v)x_4^i)) \right\},$$

that is

$$S \leqslant p^{d-1} \sum_{t_1,t_3=0}^{p-1} e(t_1+t_3) N_d(t_1, -(t_1+v), t_3, -(t_3-v)). \tag{4.4}$$

Then

$$S \leqslant p^{d-1}(\Sigma_1 + \Sigma_2 + \ldots + \Sigma_{12}), \tag{4.5}$$

https://doi.org/10.4153/CJM-1967-060-1 Published online by Cambridge University Press

where $\sum_i$ $(i = 1, 2, \ldots, 12)$ denotes the sum in (4 4) with t_1 and t_3 restricted as below:

1. $t_1 = 0,\ t_3 = 0.$
2. $t_1 = 0,\ t_3 = v.$
3. $t_1 = -v,\ t_3 = v.$
4. $t_1 = -v,\ t_3 = 0.$
5. $t_1 = 0,\ t_3 = 2^{-1}v.$
6. $t_1 = -v,\ t_3 = 2^{-1}v.$
7. $t_1 = -2^{-1}v,\ t_3 = 0.$
8. $t_1 = -2^{-1}v,\ t_3 = v.$
9. $t_1 = -2^{-1}v,\ t_3 = 2^{-1}v.$
10. $t_1 \neq 0, -v, -2^{-1}v;\ t_3 \neq 0, v, 2^{-1}v;\ t_1 + t_3 \neq 0;\ t_1 = t_3 - v.$
11. $t_1 \neq 0, -v, -2^{-1}v;\ t_3 \neq 0, v, 2^{-1}v;\ t_1 + t_3 = 0;\ t_1 \neq t_3 - v.$
12. $t_1 \neq 0, -v, -2^{-1}v;\ t_3 \neq 0, v, 2^{-1}v;\ t_1 + t_3 \neq 0;\ t_1 \neq t_3 - v.$

In Case 1

$$N_d(t_1, -(t_1+v), t_3, -(t_3-v)) = N_d(0, -v, 0, v) = p^2 N_d(-v, v) = p^3,$$

by Lemma 3.1 and so

$$\sum\nolimits_1 = p^3. \tag{4.6}$$

Cases 2, 3, and 4 are exactly similar to Case 1. We find that

$$\sum\nolimits_2 = e(v)p^3, \tag{4.7}$$

$$\sum\nolimits_3 = p^3, \tag{4.8}$$

and

$$\sum\nolimits_4 = e(-v)p^3. \tag{4.9}$$

In Case 5

$$\begin{aligned} N_d(t_1, -(t_1+v), t_3, -(t_3-v)) &= N_d(0, -v, 2^{-1}v, 2^{-1}v) \\ &= pN_d(-v, 2^{-1}v, 2^{-1}v) \\ &= p(p + O(1)) = p^2 + O(p) \end{aligned}$$

by Lemma 3.2, and so

$$\sum\nolimits_5 = e(2^{-1}v)p^2 + O(p). \tag{4.10}$$

Cases 6, 7, and 8 are exactly similar to Case 5. We find that

$$\sum\nolimits_6 = e(-2^{-1}v)p^2 + O(p), \tag{4.11}$$

$$\sum\nolimits_7 = e(-2^{-1}v)p^2 + O(p), \tag{4.12}$$

and

$$\sum\nolimits_8 = e(2^{-1}v)p^2 + O(p). \tag{4.13}$$

In Case 9

$$N_d(t_1, -(t_1 + v), t_3, -(t_3 - v)) = N_d(-2^{-1}v, -2^{-1}v, 2^{-1}v, 2^{-1}v).$$

Now by Lemma 3.2

$$N_d(-v, 2^{-1}v, 2^{-1}v) = p + O(1)$$

and by Lemma 3.1

$$N_d(0, -2^{-1}v, 2^{-1}v) = pN_d(-2^{-1}v, 2^{-1}v) = p^2.$$

Also by (3.13)

$$N_d^{(1234)}(-2^{-1}v, -2^{-1}v, 2^{-1}v, 2^{-1}v) = p.$$

Hence, by Lemma 3.3, we have

$$N_d(-2^{-1}v, -2^{-1}v, 2^{-1}v, 2^{-1}v) = 2(p + O(1)) + 4p^2 - (2p^2 + p) - 8p + 4p + O(1) = 2p^2 - p + O(1)$$

and so

$$\sum\nolimits_9 = 2p^2 - p + O(1). \tag{4.14}$$

Cases 10, 11, and 12 are exactly similar to Case 9. We find that

$$\sum\nolimits_{10} = -(e(v) + e(-v) + 1)p^2 + O(p), \tag{4.15}$$

$$\sum\nolimits_{11} = p^3 - 3p^2 + O(1), \tag{4.16}$$

and

$$\sum\nolimits_{12} = O(p^2). \tag{4.17}$$

Hence from (4.5), (4.6), . . . , (4.17) we have

$$\sum_{\substack{f \\ \deg f = d}} |S(v)|^2 = O(p^{d+2}). \tag{4.18}$$

Suppose that there are more than ηp^{d+1} polynomials of fixed degree d which satisfy

$$\max_{1 \leqslant v \leqslant p-1} |S(v)| > p^{\frac{1}{2}+\epsilon}. \tag{4.19}$$

Then

$$\sum_{\substack{f \\ \deg f = d}} \left\{ \max_{1 \leqslant v \leqslant p-1} |S(v)| \right\}^2 > p^{d+2+2\epsilon}, \tag{4.20}$$

which contradicts (4.18) for sufficiently large p; and this is true for every positive η. Hence the number of polynomials which satisfy (4.19) is $o(p^{d+1})$ and so almost all polynomials of degree d satisfy

$$\max_{1 \leqslant v \leqslant p-1} |S(v)| = O(p^{\frac{1}{2}}).$$

https://doi.org/10.4153/CJM-1967-060-1 Published online by Cambridge University Press

5. Proof of Theorem 3. We have that

$$\sum_{r=0}^{e-1} N_r N_{r+1} = \sum_{r=0}^{e-1} \left\{\frac{1}{p}\sum_{x,t=0}^{p-1} e(t(f(x)-r))\right\}\left\{\frac{1}{p}\sum_{y,u=0}^{p-1} e(u(f(y)-r-1))\right\}$$
$$= \frac{1}{p^2}\sum_{x,y,t,u=0}^{p-1} e(tf(x)+uf(y)-u)\sum_{r=0}^{e-1} e(-(t+u)r),$$

and so

$$\sum_{r=0}^{e-1} N_r N_{r+1} - \frac{e}{p^2}\sum_{\substack{x,y,t,u=0\\ t+u\equiv 0}}^{p-1} e(tf(x)+uf(y)-u)$$
$$= \frac{1}{p^2}\sum_{\substack{x,y,t,u=0\\ t+u\not\equiv 0}}^{p-1} e(tf(x)+uf(y)-u)\sum_{r=0}^{e-1} e(-(t+u)r),$$

that is

$$\left|\sum_{r=0}^{e-1} N_r N_{r+1} - \frac{e}{p}N_f\right|$$
$$= \frac{1}{p^2}\left|\sum_{v=1}^{p-1}\sum_{x,y,u=0}^{p-1} e((v-u)f(x)+uf(y)-u)\sum_{r=0}^{e-1} e(-vr)\right|$$
$$= \frac{1}{p}\left|\sum_{v=1}^{p-1}\left\{\sum_{s=0}^{p-1} N_s N_{s+1}\, e(-sv)\right\}\left\{\sum_{r=0}^{e-1} e(+vr)\right\}\right|$$
$$\leqslant \frac{1}{p}\sum_{v=1}^{p-1} |S(v)|\left|\sum_{r=0}^{e-1} e(+vr)\right|$$
$$\leqslant \frac{1}{p}\max_{1\leqslant v\leqslant p-1}|S(v)|\sum_{v=1}^{p-1}\left|\sum_{r=0}^{e-1} e(+vr)\right|$$
$$< \max_{1\leqslant v\leqslant p-1}|S(v)|\cdot\log p,$$

by a well-known result (see, for example, **(8)**). Hence

$$eN_f \leqslant \max_{1\leqslant v\leqslant p-1}|S(v)|\cdot p\log p,$$

and so by Theorems 1 and 2, for almost all polynomials of fixed degree d, we have

$$c_d\, pe \leqslant k_d\, p^{\frac{1}{2}}\cdot p\log p,$$

i.e.

$$e \leqslant k_d/c_d\, p^{\frac{1}{2}}\log p.$$

6. Conclusion. We have assumed throughout that $d \geqslant 4$. This was in fact necessary only in one place, namely Lemma 3.3. When $d = 2$, a result of Burgess **(2)** gives

(6.1) $$e = O(p^{11/24}\log^{2/3} p).$$

Concerning the case $d = 3$, the author and K. McCann plan to publish a paper on the distribution of the residues of a cubic which will include the result

$$e = O(p^{\frac{1}{2}} \log p), \tag{6.2}$$

valid for *all* cubics.

As we have only proved an "almost all" result, it would have been sufficient to prove that

$$N_f = p + O(p^{\frac{1}{2}}), \tag{6.3}$$

for almost all polynomials f. A proof of this can be given on exactly the same lines as that of Theorem 2, by showing that

$$\sum_{\substack{f \\ \deg f = d}} (N_f - p)^2 = O(p^{d+2}). \tag{6.4}$$

This, together with Theorem 2, proves Theorem 3 in a completely elementary manner but has the disadvantage of not showing the existence of e for *all* polynomials for all sufficiently large p.

We also remark that in the special case

$$f(x) = a_0 x^d$$

we have

$$\begin{aligned} S(v) &= \sum_{s=0}^{p-1} N_s N_{s+1} e(-sv) \\ &= \sum_{s=0}^{p-1} \{1 + \chi(a_0^{-1} s) + \ldots + \chi^{d-1}(a_0^{-1} s)\} \\ &\qquad\qquad \times \{1 + \chi(a_0^{-1}(s+1)) + \ldots + \chi^{d-1}(a_0^{-1}(s+1))\} e(-sv) \\ &= \sum_{i,j=0}^{d-1} \left\{ \sum_{s=0}^{p-1} \chi^i(a_0^{-1} s) \chi^j(a_0^{-1}(s+1)) e(-sv) \right\}, \end{aligned}$$

where χ denotes a dth order character (mod p) (without loss of generality $d|p-1$) and so by a result of Perel'muter **(9)**

$$S(v) = O(p^{\frac{1}{2}}).$$

Hence

$$e = O(p^{\frac{1}{2}} \log p),$$

in this special case. When $a_0 = 1$, much more is known; see for example **(4, 1)** for the cases $d = 3$ and 4 respectively.

Finally we make the following

CONJECTURE. *For all polynomials of fixed degree d, we have*

$$e = O(p^{\frac{1}{2}} \log p),$$

where the constant implied by the O-symbol depends only on d.

https://doi.org/10.4153/CJM-1967-060-1 Published online by Cambridge University Press

References

1. R. G. Bierstedt and W. H. Mills, *On the bound for a pair of consecutive quartic residues of a prime*, Proc. Amer. Math. Soc., *14* (1963), 628–632.
2. D. A. Burgess, *On Dirichlet characters of polynomials*, Proc. London Math. Soc., *13* (1963), 537–548.
3. L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J., *24* (1957), 37–41.
4. M. Dunton, *Bounds for pairs of cubic residues*, Proc. Amer. Math. Soc., *16* (1965), 330–332.
5. L-K. Hua, *Die Abschatzung von exponential Summen und ihre Anwendung in der Zahlentheorie, Enzyklopädie der Mathematischen-Wissenschaften*, vol. 1, pt. 2 (1959), p. 39.
6. S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math., *16* (1954), 819–827.
7. S. H. Min, *On systems of algebraic equations and certain exponential sums*, Quart. J. Math. Oxford, *18* (1947), 133–142.
8. L. J. Mordell, *On the least residue and non-residue of a polynomial*, J. London Math. Soc., *38* (1963), 451–453.
9. G. I. Perel'muter, *On certain sums of characters*, Uspehi Mat. Nauk, *18* (1963), 145–149.
10. A. Weil, *On the Riemann hypothesis in function fields*, Proc. Nat. Acad. Sci. U.S.A., *27* (1941), 345–347.

University of Manchester,
Manchester 13, England