ACTA ARITHMETICA
XLIII (1984)

On Dirichlet characters of polynomials*

by

A. M. NARANJANI (Teheran)

In this paper our objective is to investigate the distribution of x such that $\chi(f(x)) \neq 1$, where f is a fixed polynomial belonging to $\mathbf{Z}[x]$ and χ is a Dirichlet character of order $q \bmod p$.

1. Let q be a fixed integer, and let f be a fixed non-linear polynomial that is a product of rational linear factors and is not a perfect qth power. It was proved by D. A. Burgess [1] that if ε is any fixed positive number, if $p \equiv 1 \pmod q$ is a sufficiently large prime number and χ is a qth order character $(\bmod\, p)$, we have for all positive integers H and M satisfying

$$p^{1/4+\varepsilon} \leqslant H \leqslant p^{1/2}$$

that

$$H - \Big| \sum_{x=M+1}^{M+H} \chi(f(x)) \Big| \gg H^2 p^{-1/2}$$

the constant implied in the notation depending on ε, q, and f.

It follows that $\chi(f(x)) \neq 1$ for some x satisfying

$$0 < x < p^{1/4+\varepsilon}.$$

We extend this result as follows:

2. THEOREM. *Let $g(x)$ belong to $\mathbf{Z}[x]$ and g be invariant under the map*

$$\sigma\colon x \mapsto -x-a,$$

where a is a fixed integer. Let $a_1, \ldots, a_k, b_1, \ldots, b_t$ be integers satisfying

$$0 = b_1 < b_2 < \ldots < b_t = b,$$

$$a_1 < a_2 < \ldots < a_k \quad (k \geqslant 1)$$

and either $a_1 + a_k < a$ or $a_1 + a_k - 2b > a$.

---

* The results in this paper formed a part of the author's Ph. D. thesis, Nottingham 1980.

Let q be a fixed integer and let ε be any fixed positive number. Let

$$f(x) = \prod_{j=1}^{k} (x+a_j)^{a_j} \prod_{i=1}^{t} g(x+b_i)^{\beta_i},$$

where

$$(a_1, q) = (a_k, q) = (\beta_1, q) = (\beta_t, q) = 1.$$

Then if $p \equiv 1 \pmod q$ is a sufficiently large prime number and χ is a q-th order character $\pmod p$, for all integers H satisfying

$$p^{1/4+\varepsilon} \leqslant H \leqslant p^{1/2}$$

we have

$$2H - \Big|\sum_{x=-H}^{H} \chi\big(f(x)\big)\Big| \gg H^2 p^{-1/2},$$

the constant implied in the notation depending on ε, q, and f.

2.1. Example. $f(x) = x(x-1)(x^2+k)$, $f(x) = x(x+1)(x^2+2x-1)$, and $f(x) = x(x+1)(x^2+2x-1)(x^2-2)$ satisfy the hypothesis of the above theorem.

It is implicit in [1] that the conclusion of Theorem 2 holds for any polynomial with integral coefficients and having the following property.

3. Property. *There exist a constant A and positive constants B, C and a prime number q_1, depending on f and q, and a q_1-th order character $\chi_1 \pmod p$ such that if*

$$\chi\big(f(\pm x+y)\big) = \zeta, \quad |y| \leqslant nB+C,$$

where ζ is a q-th root of unity, then

$$\chi_1\{(x+A)^{q_1-1}(x+A+rB)\} = 1 \quad (1 \leqslant r \leqslant n).$$

Now, for the proof of Theorem 2 it is sufficient to show that the polynomial f described there has Property 3. The rest of the proof can then be completed as in [1].

4. For the moment let q be a prime number and

$$F(x) = g(x)^{\beta_1} g(x+b_2)^{\beta_2} \ldots g(x+b_t)^{\beta_t}.$$

We define an *operator* T on the finite set S of polynomials of the form

$$G(x) = g(x)^{\gamma_0} g(x+1)^{\gamma_1} \ldots g(x+b-1)^{\gamma_{b-1}} \text{(1)}$$

(1) Any $G(x)$ has at most one such representation as is seen by considering the factorization of g over C.

where each γ_i satisfies $0 \leqslant \gamma_i < q$, $\gamma_0 \neq 0$ and $b = b_t$. To define $TG(x)$ we choose h so that

$$h\beta_1 + \gamma_0 \equiv 0 \pmod q, \quad 0 < h < q,$$

and write

$$G(x)F(x)^h = g(x)^{\delta_0} \ldots g(x+b-1)^{\delta_{b-1}} g(x+b)^{\delta_b}$$

where

$$\delta_0 = h\beta_1 + \gamma_0 \equiv 0 \pmod q \quad \text{and} \quad \delta_b = h\beta_t \not\equiv 0 \pmod q.$$

Next we write

$$H(x) = \prod_{i=0}^{b} g(x+i)^{[\delta_i/q]}$$

and choose $K(x)$ so that

(1) $$G(x)F(x)^h = K(x)H(x)^q.$$

Thus, we have

$$K(x) = \prod_{i=0}^{b} g(x+i)^{\varepsilon_i},$$

where each ε_i satisfies $0 \leqslant \varepsilon_i < q$, $\varepsilon_0 = 0$, $\varepsilon_b \neq 0$. Let ε_c be the first non-zero ε_i. We define

(2) $$TG(x) = K(x-c) = g(x)^{\varepsilon_c} g(x+1)^{\varepsilon_{c+1}} \ldots g(x+b-c)^{\varepsilon_b} \in S.$$

4.1. Lemma. *T is a bijective operator on S.*

Proof. Since S is a finite set it suffices to show T is injective. Suppose that $G'(x)$ and $G''(x)$ are elements of S for which

$$TG'(x) = TG''(x) = G(x).$$

Then we may write

(3) $$G'(x)F(x)^{h'} = H'(x)^q K'(x),$$

(4) $$G''(x)F(x)^{h''} = H''(x)^q K''(x),$$

where

(5) $$K'(x-c') = K''(x-c'') = G(x) = g(x)^{\gamma_0} \ldots g(x+b-1)^{\gamma_{b-1}}.$$

We must deduce that $G'(x) = G''(x)$.

Let γ_d be the last non-zero γ_i. Since

$$K'(x) = \prod_{i=0}^{b} g(x+i)^{\varepsilon'_i}, \quad \varepsilon'_b \neq 0$$

and by (5) we have

$$K'(x) = G(x+c') = g(x+c')^{\gamma_0} \dots g(x+d+c')^{\gamma_d},$$

it follows that $d+c' = b$. Similarly, we have $d+c'' = b$. It follows immediately that $c' = c''$. Moreover, we have

$$K'(x) = G(x+c') = G(x+c'') = K''(x). \tag{6}$$

Next, by considering the exponents of $g(x+b)$ on both sides of (3), we see that

$$h'\beta_t \equiv \gamma_d \pmod{q}, \quad 0 < h' < q. \tag{7}$$

By (4) h'' also satisfies these uniquely soluble conditions. Thus we have $h' = h''$.

Now, using (3), (4), (6) and (7), we obtain

$$\frac{G'(x)}{G''(x)} = \left(\frac{H'(x)}{H''(x)}\right)^q.$$

But from their definitions

$$\frac{G'(x)}{G''(x)} = \prod_{i=0}^{b-1} g(x+i)^{\gamma_i'-\gamma_i''}$$

where $-q < \gamma_i'-\gamma_i'' < q$. Hence we must have $G'(x) = G''(x)$.

4.2. Corollary. *There exists a positive integer m such that*

$$T^m g(x) = g(x).$$

Proof. T is a permutation on the finite set S. Hence T has finite order.

For every F as in Section 4, where g and the b_j satisfy the hypotheses of Theorem 2, we have

5. Lemma. *There exist positive integers $c_1, c_2, \dots, c_m$ and $h_1, h_2, \dots, h_m$ such that $0 < h_i < q$ for each i and*

$$\prod_{n=1}^{m} \{F(x+c_1+\dots+c_{n-1})F(-x-a-c_n-\dots-c_m)\}^{h_n}$$

is a perfect q-th power, where m is as in the above corollary.

Proof. By (2) we have

$$(TG)(x+c) = K(x).$$

We choose $G(x) = (T^{n-1}g)(x)$. It follows from (1) that

$$(T^{n-1}g)(x)\{F(x)\}^{h_n} = (T^n g)(x+c_n)\{H_n(x)\}^q$$

holds identically. Next, we replace x by $x+c_1+\dots+c_{n-1}$ so that

$$(T^{n-1}g)(x+c_1+\dots+c_{n-1})\{F(x+c_1+\dots+c_{n-1})\}^{h_n}$$
$$= (T^n g)(x+c_1+\dots+c_n)\{H_n(x+c_1+\dots+c_{n-1})\}^q.$$

Choose m as in Corollary 4.2. We have

$$\prod_{n=1}^{m} (T^{n-1}g)(x+c_1+\dots+c_{n-1}) \prod_{n=1}^{m} \{F(x+c_1+\dots+c_{n-1})\}^{h_n}$$
$$= \prod_{n=1}^{m} (T^n g)(x+c_1+\dots+c_n) \Big\{\prod_{n=1}^{m} H_n(x+c_1+\dots+c_{n-1})\Big\}^q$$
$$= \prod_{n=1}^{m} (T^{n-1}g)(x+c_1+\dots+c_{n-1}) \frac{(T^m g)(x+c_1+\dots+c_m)}{(T^0 g)(x)} \{K'(x)\}^q,$$

where $K'(x) = \prod_{n=1}^{m} H_n(x+c_1+\dots+c_{n-1})$. Since $T^m g = g$, we get

$$\prod_{n=1}^{m} \{F(x+c_1+\dots+c_{n-1})\}^{h_n} = \frac{g(x+c_1+\dots+c_m)}{g(x)} \{K'(x)\}^q. \tag{8}$$

Next, we replace x by $-x-a-(c_1+\dots+c_m)$. It follows that

$$\prod_{n=1}^{m} \{F(-x-a-c_1-\dots-c_m)\}^{h_n} \tag{9}$$
$$= \frac{g(-x-a)}{g(-x-a-c_1-\dots-c_m)} \{K'(-x-a-c_1-\dots-c_m)\}^q.$$

On multiplying (8) and (9), and considering $g(x) = g(-x-a)$ identically, we obtain the result.

Proof of Theorem 2. It is enough to show that f satisfies Property 3. We do this in several steps.

Step 1. $t = 0$. This was proved by D. A. Burgess in [1].

Step 2. $t \geqslant 1$ and $a > a_1+a_k$. Let q_1 be a prime divisor of q and

$$f_1(x) = \prod_{j=1}^{k} (x+a_j)^{[\alpha_j/q_1]} \prod_{i=1}^{t} g(x+b_i)^{[\beta_i/q_1]}.$$

We write $f(x) = \{f_1(x)\}^q f_2(x)$, where

$$f_2(x) = \prod_{j=1}^{k} (x+a_j)^{\gamma_j} \prod_{i=1}^{t} g(x+b_i)^{\delta_i}, \quad 0 \leqslant \gamma_j, \delta_i < q_1, \ \gamma_1\gamma_k\delta_1\delta_t \neq 0.$$

Let

$$\chi_1 = \chi^{q/q_1}.$$

So that χ_1 is a q_1-th order character (mod p). Then, if in Lemma 5, $F(x)$ is chosen to be

$$F(x) = \frac{f_2(x)}{\prod_{j=1}^{k}(x+a_j)^{\gamma_j}} = g(x)^{\delta_1}\dots g(x+b_t)^{\delta_t},$$

it follows that there exist positive integers $c_1, c_2, \dots, c_m$ and $h_1, \dots, h_m$ such that

$$\prod_{n=1}^{m}\left(\frac{f_2(x+c_1+\dots+c_{n-1})f_2(-x-a-c_n-\dots-c_m)}{\prod_{j=1}^{k}(x+c_1+\dots+c_{n-1}+a_j)^{\gamma_j}(-x-a-c_n-\dots-c_m+a_j)^{\gamma_j}}\right)^{h_n}$$

is a perfect q_1-th power, say $\{L(x)\}^{q_1}$. Write

$$h(x) = \prod_{n=1}^{m}\prod_{j=1}^{k}[(x+c_1+\dots+c_{n-1}+a_j)(x+a+c_n+\dots+c_m-a_j)]^{\gamma_j h_n}.$$

Since $a > a_1+a_k$, we have

$$a_1 < a_j+c_1+\dots+c_{n-1} \quad (jn>1),$$
$$a_1 < a-a_k \leqslant a+c_n+\dots+c_m-a_j.$$

Therefore the factor $(x+a_1)$ occurs to the power $\gamma_1 h_1 \not\equiv 0 \pmod q$. Thus $h(x)$ is not a perfect q-th power mod p.

By the case $t=0$, we have constants $A, B>0, C>0$ such that

$$\chi_1\big(h(\pm x+y)\big) = \zeta \quad (|y| \leqslant nB+C),$$

then

$$\chi_1\big((x+A)^{q_1-1}(x+A+rB)\big) = 1 \quad (1 \leqslant r \leqslant n).$$

Now if

$$\chi\big(f(\pm x+y)\big) = \zeta \quad (|y| \leqslant nB+C+|a|+c_1+\dots+c_m),$$

then, since

$$\chi_1\big(f_2(\pm x+y)\big) = \chi_1\big(f_1(\pm x+y)^{q_1}\big)\chi_1\big(f_2(\pm x+y)\big) = \chi_1\big(f(\pm x+y)\big) = \chi\big(f(\pm x+y)\big)^{q/q_1} = \zeta^{q/q_1},$$

we have

$$\chi_1\big(h(\pm x+y)\big) = \big(\chi_1(-1)\big)^{\Sigma\Sigma\gamma_j h_n}\times$$
$$\times\prod_{n=1}^{m}\{\chi_1\big(f_2(\pm x+c_1+\dots+c_{n-1}+y)\big)\chi_1\big(f_2(\pm x-a-c_n-\dots-c_m-y)\big)\}^{h_n}$$
$$= \big(\chi_1(-1)\big)^{\Sigma\Sigma\gamma_j h_n}\zeta^{2q/q_1^{\Sigma h_n}} \quad (|y| \leqslant nB+C)$$

whence the result follows immediately.

Step 3. $t \geqslant 1$, and $a_1+a_k-2b > a$. We write

$$f_1(x) = f(-x-a-b)(-1)^{\Sigma a_j}$$
$$= \prod_{j=1}^{k}\big((-x-a-b+a_j)(-1)\big)^{a_j}\prod_{i=1}^{t} g(-x-a-b+b_i)^{\beta_i}.$$

Then if

$$f_1(x) = \prod_{j=1}^{k}(x+a_j')^{a_j}\prod_{i=1}^{t} g(x+b_i')^{\beta_i},$$

where $a_j' = a+b-a_{k-(j-1)}$, $b_i' = b-b_{t-(i-1)}$ and

$$a_1'+a_k' = a-(a_1+a_k-2b-a) < a,$$
$$0 = b_1' < b_2' < \dots < b_t',$$
$$a_1' < a_2' < \dots < a_k',$$

then by step 2, $f_1(x)$ satisfies Property 3. That is, there exist constants A, and B, $C>0$ such that if

$$\chi\big(f_1(\pm x+y)\big) = \zeta \quad (|y| \leqslant nB+C),$$

then

$$\chi_1\{(x+A)^{q_1-1}(x+A+rB)\} = 1 \quad (1 \leqslant r \leqslant n).$$

Now, if

$$\chi\big(f(\pm x+y)\big) = \zeta \quad (|y| \leqslant nB+C+|a|+b),$$

then

$$\chi\big(f_1(x)\big) = \zeta\chi(-1)^{\Sigma a_j} \quad (|y| \leqslant nB+C).$$

Hence the result follows.

Reference

[1] D. A. Burgess, *On Dirichlet characters of polynomials*, Proc. London Math. Soc. (3) 13 (1963), pp. 537–548.

DEPARTMENT OF MATHEMATICS
UNIVERSITY FOR TEACHER EDUCATION
49 Mobarezan Ave., Teheran, Iran

Received on 23. 3. 1982
and in revised form on 28. 9. 1982 (1297)