Conspectus materiae tomi LI, fasciculi 3

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-08168-6 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
LI (1988)

On the congruence $f(x^k) \equiv 0 \bmod q$, where q is a prime and f is a polynomial

by

J. Wójcik (Warszawa)

The aim of this paper is to prove the following theorems:

Theorem 1. *Let α be an algebraic number different from zero and not a root of unity. Let n be its degree. Let k be an arbitrary natural number. We have*

$$\alpha = \beta^{n_1}\gamma^{n_1}, \tag{1}$$

where $n_1 = (k, c(\alpha))$, β is cyclotomic, $\gamma \in Q(\alpha)$.

Further, let K_0 denote the maximal cyclotomic subfield of $Q(\alpha)$ and put $K_1 = K_0(\beta)$. Let f_1 be the conductor of K_1 and G_1 the group of rationals $\bmod f_1$ corresponding to K_1. Put $G_2 = G_1 \cap E_k$. The group G_2 is uniquely determined by the algebraic number α and the positive integer k. For any positive integers D and r such that $(D, r) = 1$ and the residue class of $r \bmod D$ contains a rational integer belonging to G_2 there exist infinitely many prime ideals $\mathfrak{q}$ of $Q(\alpha)$ such that α is k-th power residue $\bmod \mathfrak{q}$, $N\mathfrak{q} \equiv r \bmod D$, $N\mathfrak{q} \equiv 1 \bmod k$. The Dirichlet density of this set of prime ideals is equal to

$$\frac{n(k, c(\alpha))}{C(\alpha)k\varphi([D, k])}\frac{|K_1 \cap P_{[D,k]}|}{|K_1|}.$$

The meaning of $c(\alpha)$ and $C(\alpha)$ is explained later.

Theorem 2. *Let f be a polynomial with rational integral coefficients, irreducible, primitive, with a positive leading coefficient. Assume that f is different from x and f is not a cyclotomic polynomial. Let k be any positive integer. Let α be any root of f. We have*

$$\alpha = \beta^{n_1}\gamma^{n_1}, \tag{2}$$

where $n_1 = (k, c(f))$, β is cyclotomic, $\gamma \in Q(\alpha)$.

Further, let K_0 denote the maximal cyclotomic subfield of $Q(\alpha)$ and put $K_1 = K_0(\beta)$. Let f_1 be the conductor of K_1 and G_1 the group of rationals $\bmod f_1$ corresponding to K_1. Put $G_2 = G_1 \cap E_k$. The group G_2 is uniquely determined by the polynomial f and the positive integer k. For any positive integers D and r such that $(D, r) = 1$ and the residue class of $r \bmod D$ contains a rational integer *belonging to G_2 there exist infinitely many primes q such that $q \equiv r \bmod D$, $q \equiv 1 \bmod k$ and the congruence $f(x^k) \equiv 0 \bmod q$ is solvable in $x \in \boldsymbol{Z}$. The Dirichlet density δ of this set of primes satisfies the inequality*

$$\frac{(k, c(f))}{C(f)k\varphi([D, k])}\frac{|K_1 \cap P_{[D,k]}|}{|K_1|} \leqslant \delta \leqslant \frac{n}{\varkappa}\frac{(k, c(f))}{C(f)k\varphi([D, k])}\frac{|K_1 \cap P_{[D,k]}|}{|K_1|},$$

where

$$\varkappa = \begin{cases} 1 & \text{if } f \text{ is not reciprocal,} \\ 2 & \text{otherwise,} \end{cases}$$

n is degree of f. The meaning of $c(f)$ and $C(f)$ is explained later.

In [2], we proved Theorem 2 with the additional assumption that f is k-normal obtaining a stronger assertion on δ:

$$\delta = \frac{(k, c(f))}{C(f)k\varphi([D, k])}\frac{|K_1 \cap P_{[D,k]}|}{|K_1|}.$$

Notation. $\zeta_m = e^{2\pi i/m}$, K denotes an algebraic number field. $P_m = Q(\zeta_m)$. If $\alpha \in K$, $\zeta_m \in K$, $\alpha \neq 0$, $\mathfrak{b}$ is a fractional ideal of K then $\left(\frac{\alpha|K}{\mathfrak{b}}\right)_m$ is the mth power residue symbol. $D(\alpha)$ denotes the discriminant of α. If the extension K/Ω is abelian, then $f(K/\Omega)$ is its conductor. $f_\alpha = f(K(\sqrt[m]{\alpha})/K)$. f_α is also the conductor of $\left(\frac{\alpha|K}{\mathfrak{b}}\right)_m$. E_m is the group of rationals congruent to 1 mod m. We call a set $G \subseteq Q$ a *group of rationals* mod m if (i) $E_m \subseteq G$, (ii) G is a multiplicative group and (iii) every element of G is prime to m (clearly G/E_m is a group of residue classes mod m). If $K \subseteq P_m$ then a group G of rationals mod m is said *to correspond to* K if G/E_m is the maximal subgroup of $\mathrm{Gal}(P_m/Q)$ which leaves K fixed. $[,]$ denotes the least common multiple. $|K| = (K: Q)$. For a finite set S, $|S|$ is its cardinality. K^{mc} denotes the maximal cyclotomic extension of K. Let $\alpha \in K^{\mathrm{mc}}$. Consider the equation in unknowns n, β

$$\alpha = \beta^n, \quad n \text{ natural}, \ \beta \in K^{\mathrm{mc}} \tag{3}$$

Put

$$C_K(\alpha) = \begin{cases} \text{maximal } n \text{ satisfying (3)} & \text{if the equation (3) has only a finite number of solutions,} \\ \infty \quad \text{otherwise.} \end{cases}$$

Let f be an arbitrary polynomial with rational coefficients irreducible over Q and let α be a root of f. Put

$$c(f) = c(\alpha) = c_{Q(\alpha)}(\alpha), \quad C(f) = C(\alpha) = \big(Q(\alpha): K_0\big) = n/|K_0|$$

where n denotes the degree of f and K_0 is the maximal cyclotomic subfield of $Q(\alpha)$.

LEMMA 1. *Let α be an algebraic number different from zero and not a root of unity. Then (1) holds. Put $k_1 = Q(\alpha)$, $k_2 = k_1 P_k(\beta)$. Let K_0, K_1, f_1, G_1, G_2 have the same meaning as in Theorem 1. Let D be an arbitrary positive integer and F an arbitrary positive integer divisible by $kf_1 D$ and by the conductor of the power residue symbol $\left(\frac{\alpha|k_2}{\mathfrak{a}}\right)_k$. We have*

$$k_2 \cap P_F = K_1 P_k = k_2 \cap Q^{\mathrm{mc}}.$$

Let $r \in G_2$. There exists an ideal $\mathfrak{a}_1$ of k_2 such that

$$(\mathfrak{a}_1, F) = 1, \quad N\mathfrak{a}_1 \equiv r \bmod F, \quad \left(\frac{\alpha}{\mathfrak{a}_1}\right)_k = 1.$$

The group G_2 is uniquely determined by the algebraic number α and the positive integer k.

Proof. See [2], p. 155–156. We only have to prove the last statement of the lemma. Assume that we also have

$$\alpha = \beta'^{n_1}\gamma'^{n_1}, \quad \beta' \in Q^{\mathrm{mc}}, \ \gamma' \in Q(\alpha).$$

We have

$$\alpha = \beta_1'^{n_1}, \quad \beta_1' = \beta'\gamma', \quad \alpha = \beta_1^{n_1}, \quad \beta_1 = \beta\gamma.$$

By Lemma 4 of [2] $K_0(\beta) = K_0 Q(\beta)$ is the maximal cyclotomic subfield of the field $k_1 Q(\beta) = k_1(\beta) = k_1(\beta_1) = Q(\beta_1)$. Analogously, $K_0(\beta')$ is the maximal cyclotomic subfield of the field $Q(\beta_1')$. We have

$$\beta_1' = \zeta_{n_1}^a \beta_1 \quad \text{and} \quad Q(\beta_1')P_k = Q(\zeta_{n_1}^a \beta_1)P_k = Q(\beta_1)P_k (n_1|k).$$

Put $K_1' = K_0(\beta')$. Hence by Lemma 4 of [2]

$$K_1' P_k = K_0(\beta')P_k = K_0(\beta)P_k = K_1 P_k.$$

This means that $K_1 P_k$ is uniquely determined by the algebraic number α and by the positive integer k. $[k, f_1]$ is uniquely determined by α and k. Since G_2 is the group of rationals mod $[k, f_1]$ corresponding to $K_1 P_k$, G_2 is uniquely determined by k and by α.

LEMMA 2. *Let*

$$C = \left\{\mathfrak{a}\colon \mathfrak{a} \text{ an ideal of } k_2,\ (\mathfrak{a}, F) = 1,\ N\mathfrak{a} \equiv r \bmod F,\ \left(\frac{\alpha}{\mathfrak{a}}\right)_k = 1\right\},$$

where $(r, F) = 1$, $r \in G_2$,

$$C' = \{\mathfrak{q}_1\colon \mathfrak{q}_1 \text{ a prime ideal of } k_1;\ N\mathfrak{q}_1 \equiv r \bmod F,\ \alpha \text{ is a } k\text{-th power residue} \bmod \mathfrak{q}_1\},$$

where $(r, F) = 1$, $r \in G_2$.

Then if $\mathfrak{q}_2 \in C$ is a prime ideal of k_2 of degree one over k_1 and $N\mathfrak{q}_2$ is sufficiently large then there exist exactly $|k_2|/|k_1|$ prime ideals $\tau\mathfrak{q}_2$ $(\tau \in G(k_2/k_1))$ of degree one over k_1 belonging to C and dividing a certain prime ideal $\mathfrak{q}_1$ of k_1 belonging to C' $(\mathfrak{q}_1 = N_{k_2/k_1}\mathfrak{q}_2)$. Conversely, if $\mathfrak{q}_1 \in C'$ is a prime ideal of k_1 and $N\mathfrak{q}_1$ is sufficiently large, then $\mathfrak{q}_1$ splits completely in k_2 and each of its prime divisors $\mathfrak{q}_2$ in k_2 belongs to C.

Proof. See [1], p. 160. By Lemma 1 the set C is non empty. We only have to prove that if $\mathfrak{q}_1 \in C'$ is a prime ideal of k_1 and $N\mathfrak{q}_1$ is sufficiently large, then $\mathfrak{q}_1$ splits completely in k_2. Put $f_2 = [k, f_1]$. We have $k_2 = k_1 P_k(\beta) = k_1 Q(\beta) P_k = k_1 K_1 P_k$. We have $K_1 P_k = Q(\xi)$, ξ an integer, $k_2 = k_1(\xi)$. Let $N\mathfrak{q}_1 = q^{f_3} \in G_2$. We have $K_1 P_k \subseteq P_{f_2}$. Hence $\xi = h(\zeta_{f_2})$, $h \in Q[x]$. Since $N\mathfrak{q}_1$ is sufficiently large, we have

$$\xi^{N\mathfrak{q}_1} \equiv h(\zeta_{f_2}^{q^{f_3}}) \equiv h(\zeta_{f_2}) \equiv \xi \bmod \mathfrak{Q}, \tag{4}$$

because G_2 is the group of rationals mod f_2 corresponding to the field $K_1 P_k$, where $\mathfrak{Q}|\mathfrak{q}_1$, $\mathfrak{Q}$ is a prime ideal of k_2. Let η be an arbitrary integer of k_2. We have

$$\eta = \sum_i a_i \xi^i, \quad a_i \in k_1.$$

By Fermat's theorem, $a_i^{N\mathfrak{q}_1} \equiv a_i \bmod \mathfrak{Q}$. Hence by (4)

$$\eta^{N\mathfrak{q}_1} \equiv \sum_i a_i^{N\mathfrak{q}_1} \xi^{iN\mathfrak{q}_1} \equiv \sum_i a_i \xi^i \equiv \eta \bmod \mathfrak{Q}.$$

This means that $\mathfrak{q}_1$ splits completely in k_2. The lemma is proved.

Proof of Theorem 1. Put

$$A = \{\mathfrak{a}\colon \mathfrak{a} \text{ an ideal of } k_2,\ (\mathfrak{a}, F) = 1\},$$

$$H_1 = \{\mathfrak{a}\colon \mathfrak{a} \text{ an ideal of } k_2,\ (\mathfrak{a}, F) = 1,\ N\mathfrak{a} \equiv 1 \bmod F\},$$

$$H = \left\{\mathfrak{a}\colon \mathfrak{a} \text{ an ideal of } k_2,\ (\mathfrak{a}, F) = 1,\ N\mathfrak{a} \equiv 1 \bmod F,\ \left(\frac{\alpha}{\mathfrak{a}}\right)_k = 1\right\},$$

$$h = (A : H).$$

By Lemma 2 and Hecke's theorem

$$\frac{1}{h} = d(C) = \lim_{s \to 1+0} \frac{\sum_{\mathfrak{q}_2 \in C} \left(\frac{1}{N\mathfrak{q}_2}\right)^s}{\log \frac{1}{s-1}} = (|k_2|/|k_1|) \lim_{s \to 1+0} \frac{\sum_{\mathfrak{q}_1 \in C'} \left(\frac{1}{N\mathfrak{q}_1}\right)^s}{\log \frac{1}{s-1}} = (|k_2|/n) d(C'), \tag{5}$$

$(|k_1| = n)$, where $\mathfrak{q}_2$ are prime ideals of k_2 of degree one over k_1.

Hence

$$d(C') = \frac{n}{h|k_2|}. \tag{6}$$

By Lemma 1 and by the argument of [2], p. 158 we have

$$d(C') = \frac{n(k, c(\alpha))}{C(\alpha) k \varphi(F)}. \tag{7}$$

Assume first that $D \equiv 0 \bmod [k, f_1]$. Put

$C'' = \{\mathfrak{q}\colon \mathfrak{q}$ a prime ideal of k_1, $N\mathfrak{q} \equiv r \bmod D$, $N\mathfrak{q} \equiv 1 \bmod k$, α is a kth power residue mod $\mathfrak{q}\}$,

where $(r, D) = 1$ and $r \in G_2$.

By the argument of [2], p. 158–159, we have

$$d(C'') = \frac{n(k, c(\alpha))}{C(\alpha) k \varphi(D)}. \tag{8}$$

Thus we have proved the theorem for $D \equiv 0 \bmod [k, f_1]$.

Let $G_1 = r_1 E_{f_1} \cup r_2 E_{f_1} \cup \ldots \cup r_t E_{f_1}$, $t = (G_1 : E_{f_1})$. Let D be any positive integer. Put

$C_j = \{\mathfrak{q}\colon \mathfrak{q}$ a prime ideal of k_1, $N\mathfrak{q} \equiv r \bmod D$, $N\mathfrak{q} \equiv 1 \bmod k$, $N\mathfrak{q} \equiv r_j \bmod f_1$, α is a kth power residue mod $\mathfrak{q}\}$,

where $(r, D) = 1$ and there exists a rational integer r'_j such tat

$$r'_j \equiv \begin{cases} r \bmod D, \\ 1 \bmod K, \\ r_j \bmod f_1. \end{cases} \tag{9}$$

Obviously

$C_j = \{\mathfrak{q}\colon \mathfrak{q}$ a prime ideal of k_1, $N\mathfrak{q} \equiv r'_j \bmod [D, k, f_1]$, α is a kth power residue mod $\mathfrak{q}\}$,

where $(r'_j, [D, k, f_1]) = 1$ and $r'_j \in G_2$.

By (8) (the theorem for $D \equiv 0 \bmod [k, f_1]$),

$$d(C_j) = \frac{n(k, c(\alpha))}{C(\alpha) k \varphi([D, k, f_1])}. \tag{10}$$

Put

$C''' = \{\mathfrak{q}\colon \mathfrak{q}$ a prime ideal of k_1, $N\mathfrak{q} \equiv r \bmod D$, $N \equiv 1 \bmod k$, α is a kth power residue mod $\mathfrak{q}\}$,

where $(r, D) = 1$ and the residue class of r mod D contains a number belonging to G_2. By the argument of [2], p. 159–160, we have

$$d(C''') = \frac{n(k, c(\alpha))}{C(\alpha) k \varphi([D, k])} \frac{|K_1 \cap P_{[D,k]}|}{|K_1|}.$$

The theorem is proved.

Proof of Theorem 2. Let $f(x) = a_0 x^n + \ldots + a_n$ be a polynomial satisfying the assumptions of the theorem. Let α be any of its roots. By the assumptions, α is different from zero and is not a root of unity. Put $k_1 = Q(\alpha)$. By Theorem 1 we have (2), since $c_{k_1}(\alpha) = c(\alpha) = c(f)$. From the Theorem of [2] and the remark at the end of that paper it follows that the group G_2 is uniquely determined by the polynomial f and the positive integer k. Put

$C = \{\mathfrak{q}$: $\mathfrak{q}$ a prime ideal of k_1, $N\mathfrak{q} \equiv 1 \bmod k$, $N\mathfrak{q} \equiv r \bmod D$, α is a kth power residue $\bmod \mathfrak{q}\}$,

$B = \{q$: q a prime number, $q \equiv 1 \bmod k$, $q \equiv r \bmod D$, the congruence $f(x^k) \equiv 0 \bmod q$ is solvable$\}$,

where $(r, D) = 1$ and residue class of $r \bmod D$ contains a rational integer belonging to G_2.

By the same argument as in [1] we have

$$\frac{1}{n} d(C) \leqslant d(B) \leqslant \frac{1}{\varkappa} d(C). \tag{11}$$

By the definition of $c(f)$ and $C(f)$, $c(\alpha) = c(f)$, $C(\alpha) = C(f)$. Hence by Theorem 1

$$d(C) = \frac{n(k, c(f))}{C(f) k\varphi([D, k])} \frac{|K_1 \cap P_{[D,k]}|}{|K_1|}.$$

By (11)

$$\frac{(k, c(f))}{C(f) k\varphi([D, k])} \frac{|K_1 \cap P_{[D,k]}|}{|K_1|} \leqslant d(B) \leqslant \frac{n}{\varkappa} \frac{(k, c(f))}{C(f) k\varphi([D, k])} \frac{|K_1 \cap P_{[D,k]}|}{|K_1|}.$$

Theorem 2 is proved.

References

[1] J. Wójcik, *Contributions to the theory of Kummar extensions*, Acta Arith. 40 (1982), 155–174.

[2] — *On the congruence $f(x^k) \equiv 0 \bmod q$, where q is a prime and f is a k-normal polynomial*, ibid. 41 (1982), 151–161.

Received on 22.11.1985
and in revised form on 9.1.1987 (1563)

ACTA ARITHMETICA
LI (1988)

Multiplicative functions and Brun's sieve

by

KRISHNASWAMI ALLADI (Gainesville, Florida)

1. Introduction. Let g be a strongly multiplicative function. That is

$$g(n) = \prod_{\substack{p \mid n \\ p = \text{prime}}} g(p).$$

The *truncation* of g at y is

$$g_y(n) = \prod_{\substack{p \mid n \\ p < y}} g(p).$$

As is customary null products have value one.

For any set $\mathscr{A}$ of positive integers we let $\mathscr{A}(x)$ denote $\mathscr{A} \cap [1, x]$. The problem we consider here is the estimation of

$$S_g(\mathscr{A}(x), y) = \sum_{n \in \mathscr{A}(x)} g_y(n) \tag{1.1}$$

for sets $\mathscr{A}$ satisfying certain conditions to be specified in Section 2. We were motivated to study this sum because it turns out (as will be seen in Section 3) to be a natural generalization of a typical sieve problem. We show that Brun's sieve could be used to estimate $S_g(\mathscr{A}(x), y)$ when $-1 \leqslant g \leqslant 1$, provided $\alpha = (\log|\mathscr{A}(x)|)/\log y$ is not small (see § 5–§ 7) and for this we make use of an interesting 'monotonicity principle' (see § 4).

Previously [1], [2], [3] we had investigated such sums when $0 < g \leqslant 1$. In this case g may be written as

$$g(n) = e^{uf(n)}$$

where $u < 0$ and $f \geqslant 0$ is a strongly additive function. So the sum in (1.1) can be interpreted in terms of the Laplace transform of f_y, which is the truncation of f and y. Such an approach led to a new method of estimating the moments of f using the sieve. For the sake of completeness we shall state (without proof) towards the end of Section 6 some results for the case $0 \leqslant g \leqslant 1$ but in a slightly stronger form than was utilized by us earlier. The main interest in the present paper lies in showing that the sieve can be employed to deal with such