On the congruence \( f(x^q) \equiv 0 \mod q \), 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 \( \alpha \) 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

\[
\alpha = \beta n^{\gamma},
\]

where \( n = (k, c(\alpha)) \), \( \beta \) is cyclotomic, \( \gamma \in \mathbb{Q}(\alpha) \).

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

\[
\frac{n(k, c(\alpha))}{C(\alpha)kp([D, k])} [K_1 : \mathbb{Q}(\alpha)] [K_1 : \mathbb{Q}].
\]

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 \( \alpha \) be any root of \( f \). We have

\[
\alpha = \beta n^{\gamma},
\]

where \( n = (k, c(f)) \), \( \beta \) is cyclotomic, \( \gamma \in \mathbb{Q}(\alpha) \).

Further, let \( K_0 \) denote the maximal cyclotomic subfield of \( \mathbb{Q}(\alpha) \) and put \( K_1 = K_0(\beta) \). Let \( f_1 \) be the conductor of \( K_1 \) and \( G_1 \) the group of rationals \( \mod f_1 \) 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 \( r \mod D \) contains a rational integer...
belonging to \( G_2 \) there exist infinitely many primes \( q \) such that \( q \equiv r \mod D \), \( q \equiv 1 \mod k \) and the congruence \( f(x^q) \equiv 0 \mod q \) is solvable in \( x \in \mathbb{Z} \). The Dirichlet density \( \delta \) of this set of primes satisfies the inequality

\[
\frac{(k, c(f))}{C(f)k\varphi([D, k])} \leq \delta \leq \frac{\varphi([D, k])}{|K_1|}.
\]

where

\[ \varphi([D, k]) \]

is the 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 \( \delta \):

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

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

\[
\alpha = \beta^n, \quad n \text{ natural}, \quad \beta \in K^{\text{cyc}}
\]

(3)

Put

\[
C_\mathbb{Q}(\alpha) = \left\{ \begin{array}{ll}
\text{maximal } n \text{ satisfying (3)} & \text{ if the equation (3) has only a finite number of solutions,} \\
\infty & \text{ otherwise.}
\end{array} \right.
\]

Let \( f \) be an arbitrary polynomial with rational coefficients irreducible over \( Q \) and let \( \alpha \) be a root of \( f \). Put

\[
c(f) = c(\alpha) = C_\mathbb{Q}(\alpha), \quad C(f) = C(\alpha) = (Q(\alpha): K_0) = n/K_0
\]

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

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

\[
k_2 \cap P_{F} = K_1 P_{F} = k_2 \cap Q^{\text{cyc}}.
\]

Let \( r \in G_2 \). There exists an ideal \( \alpha_1 \) of \( k_2 \) such that

\[
\left( \frac{\alpha_1}{k_1} \right)_k = 1.
\]

The group \( G_2 \) is uniquely determined by the algebraic number \( \alpha \) 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

\[
\alpha = \beta^\gamma, \quad \beta' \in Q^{\text{cyc}}, \quad \gamma' \in Q(\alpha).
\]

We have

\[
\alpha = \beta^n, \quad \beta'_1 = \beta' \gamma', \quad \alpha = \beta^n, \quad \beta_1 = \beta\gamma.
\]

By Lemma 4 of [2] \( K_0(\beta) = K_0(\beta') \) is the maximal cyclotomic subfield of the field \( k_1 \mathbb{Q}(\beta) = k_1(\beta) = k_1(\beta_1) = Q(\beta_1) \). Analogously, \( K_0(\beta') \) is the maximal cyclotomic subfield of the field \( Q(\beta'_1) \). We have

\[
\beta'_1 = \zeta_m, \quad \text{ and } \quad Q(\beta'_1)_P = Q(\mathbb{Q}, \beta_1)_P = Q(\beta_1) P_{k_1|k}.
\]

Put \( K'_1 = K_0(\beta'_1) \). Hence by Lemma 4 of [2]

\[
K'_1 P_{k_1} = K_0(\beta') P_{k_1} = K_0(\beta') P_{k_1}.
\]

This means that \( K_1 P_{k_1} \) is uniquely determined by the algebraic number \( \alpha \) and by the positive integer \( k_1 \). \( k_1, f_1 \) is uniquely determined by \( \alpha \) and \( k_1 \). Since \( G_2 \) is the group of rationals \( m \mod m \) corresponding to \( K_1 P_{k_1} \), \( G_2 \) is uniquely determined by \( k_1 \) and by \( \alpha \).

**Lemma 2.** Let

\[
C = \left\{ a : a \text{ an ideal of } k_2, (\alpha, F) = 1, N\alpha \equiv r \mod F, \left( \frac{\alpha}{N\alpha} \right)_k = 1 \right\},
\]

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

\[
C' = \{ a_1 : a_1 \text{ a prime ideal of } k_1, N\alpha_1 \equiv r \mod F, \alpha \text{ is a } k-\text{th power residue } \mod q_1 \},
\]

where \( (r, F) = 1, r \in G_2 \).
Then if \(a_1 \in C\) is a prime ideal of \(k_2\) of degree one over \(k_1\), and \(Nq_2\) is sufficiently large then there exist exactly \(|k_2|/|k_1|\) prime ideals \(q_2\) (\(r \in G(k_2/k_1)\)) of degree one over \(k_1\) belonging to \(C\) and dividing a certain prime ideal \(q_1\) of \(k_1\) belonging to \(C\) (\(q_1 = Nq_2a_1q_2\)). Conversely, if \(q_1 \in C\) is a prime ideal of \(k_1\) and \(Nq_1\) is sufficiently large, then \(q_1\) splits completely in \(k_2\) and each of its prime divisors \(q_2\) 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 \(q_1 \in C\) is a prime ideal of \(k_1\) and \(Nq_1\) is sufficiently large, then \(q_1\) splits completely in \(k_2\). Put \(f_2 = [k_2, f_2]\). We have \(k_2 = k_1 P_2 = k_1 Q(\xi) P_{k_2} = k_1 K_2 P_k\). We have \(K_2 P_k = \mathbb{Q}(\xi)\), \(k_2 = k_2(\xi)\). Let \(Nq_1 = q_1 f_2 \in G_2\). We have \(K_2 P_k \subseteq P_{f_2}\). Hence \(\xi = h(f_2), h \in \mathbb{Q}[x]\). Since \(Nq_1\) is sufficiently large, we have

\[
\xi^{Nq_1} = h(f_2)^{Nq_1} \equiv h(f_2) \equiv \xi \mod \mathfrak{Q},
\]

because \(G_2\) is the group of rationals mod \(f_2\) corresponding to the field \(K_2 P_k\), where \(Q/\mathfrak{Q}\), \(\mathfrak{Q}\) is a prime ideal of \(k_2\). Let \(\eta\) be an arbitrary integer of \(k_2\).

\[
\eta = \sum_{i} a_i \xi^i, \quad a_i \in k_1.
\]

By Fermat's theorem, \(a_i^{Nq_1} \equiv a_i \mod \mathfrak{Q}\). Hence by (4)

\[
\eta^{Nq_1} \equiv \sum_{i} a_i^{Nq_1} \xi^{Nq_1} \equiv \sum_{i} a_i \xi^i \equiv \eta \mod \mathfrak{Q}.
\]

This means that \(q_1\) splits completely in \(k_2\). The lemma is proved.

**Proof of Theorem 1.** Put

\[
A = \{a: \text{a an ideal of } k_2, (a, F) = 1\},
\]

\[
H_1 = \{a: \text{a an ideal of } k_2, (a, F) = 1, Nq_1 \equiv 1 \mod F\},
\]

\[
H = \{a: \text{a an ideal of } k_2, (a, F) = 1, Nq_1 \equiv 1 \mod F, \left(\frac{a}{k_1}\right) = 1\},
\]

\[
h = (A: H).
\]

By Lemma 2 and Hecke's theorem

\[
\frac{1}{h} = d(C) = \lim_{s \to 1+0} \frac{1}{|Nq_2|} \log \frac{1}{|k_2|/|k_1|} = \lim_{s \to 1+0} \frac{1}{|Nq_1|} \log \frac{1}{|k_2|/|k_1|} = \llbracket k_2/|k_1| \rrbracket d(C),
\]

\(|k_1| = n\), where \(q_2\) are prime ideals of \(k_2\) of degree one over \(k_1\).

Hence

\[
d(C) = \frac{n}{\llbracket k_2/|k_1| \rrbracket}.
\]

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

\[
d(C) = \frac{n(k, c(a))}{C(a)k\varphi(|F|)}.
\]

Assume first that \(D \equiv 0 \mod [k, f_1]\). Put

\[
C'' = \{q: q \text{ a prime ideal of } k_1, Nq \equiv r \mod D, Nq \equiv 1 \mod k, \alpha \text{ is a } k\text{th power residue mod } q_1\},
\]

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

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

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

Thus we have proved the theorem for \(D \equiv 0 \mod [k, f_1]\).

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

\[
C_j = \{q: q \text{ a prime ideal of } k_1, Nq \equiv r_j \mod D, Nq \equiv 1 \mod k, Nq \equiv r_j \mod f_1, \alpha \text{ is a } k\text{th power residue mod } q_1\},
\]

where \((r_j, D) = 1\) and there exists a rational integer \(r_j\) such that

\[
r_j \equiv \begin{cases} r \mod D, \\ 1 \mod K, \\ r_j \mod f_1. \end{cases}
\]

Obviously

\[
C_j = \{q: q \text{ a prime ideal of } k_1, Nq \equiv r_j \mod [D, k, f_1], \alpha \text{ is a } k\text{th power residue mod } q_1\},
\]

where \((r_j, [D, k, f_1]) = 1\) and \(r_j \in G_2\).

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

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

Put

\[
C'' = \{q: q \text{ a prime ideal of } k_1, Nq \equiv r \mod D, Nq \equiv 1 \mod k, \alpha \text{ is a } k\text{th power residue mod } q_1\},
\]

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

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

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 \( \alpha \) be any of its roots. By the assumptions, \( \alpha \) is different from zero and is not a root of unity. Put \( k_1 = Q(\alpha) \).

By Theorem 1 we have (2), since \( c_1(\alpha) = c(\alpha) = c(f) \). 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
\[
C = \{ q \in \text{prime ideal of } k_1, Nq \equiv 1 \mod k, Nq \equiv r \mod D, \alpha \text{ is a } k \text{th power residue } \mod q \},
\]
\[
B = \{ q \in \text{prime number, } q \equiv 1 \mod k, q \equiv r \mod D, \text{the congruence } f(x^q) \equiv 0 \mod q \text{ is solvable} \},
\]
where \( (r, D) = 1 \) and residue class of \( r \mod D \) contains a rational integer belonging to \( G_2 \).

By the same argument as in [1] we have
\[
\frac{1}{n} d(C) \leq d(B) \leq \frac{1}{n} d(C).
\]

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

Theorem 2 is proved.

References


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

Received on 22.11.1982
and in revised form on 9.1.1987

Multiplicative functions and Brun’s sieve

by

KRISHNASWAMI ALLADI (Gainesville, Florida)

1. Introduction. Let \( g \) be a strongly multiplicative function. That is
\[
g(n) = \prod_{\substack{p \mid n \leq \text{prime} \quad \text{prime} \leq n \leq p \leq \text{prime}}} g(p).
\]

The truncation of \( g \) at \( y \) is
\[
g_y(n) = \prod_{\substack{p \leq y \quad \text{prime}}} g(p).
\]

As is customary null products have value one.

For any set \( \mathcal{A} \) of positive integers we let \( \mathcal{A}(x) \) denote \( \mathcal{A} \cap [1, x] \). The problem we consider here is the estimation of
\[
S_y(\mathcal{A}(x), y) = \sum_{n \leq x \in \mathcal{A}(x)} g_y(n)
\]

for sets \( \mathcal{A} \) 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 \( S_y(\mathcal{A}(x), y) \) when \(-1 \leq g \leq 1\), provided \( x = (\log |\mathcal{A}(x)|)/\log y \) 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 \( 0 < g \leq 1 \). In this case \( g \) may be written as
\[
g(n) = e^{\sigma f(n)}
\]

where \( u < 0 \) and \( f > 0 \) is a strongly additive function. So the sum in (1.1) can be interpreted in terms of the Laplace transform of \( f \), 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 \( 0 \leq g \leq 1 \) 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