numbers. Using the hypothetical analogs of Theorem 2.2 and (3), we find

$$P'_a(x) \approx \sum_{t\leqslant x} P_{a,t}(x) \approx d''_a C(x)\log x \tag{4}$$

for some $d''_a > 0$. Our estimate for $C_t(x)$ should hold only for small t, but presumably the sum in (4) could be cut off at some point much less than x because those n with small $l_a(n)$ can be shown to be negligible. An approximate equality like (4) for $a = 2$ was noticed in [5].

Empirical data in [5] suggests that almost all pseudoprimes to base a are squarefree, that is $P_a(x) \sim P'_a(x)$ as $x\to\infty$, where $P_a(x)$ is the number of pseudoprimes to base a up to x. In a forthcoming paper, Pomerance shows that $P_2(x)/\log x$ is unbounded. From $P_2(x) \sim P'_2(x)$ and (4) it would follow that there are infinitely many Carmichael numbers.

References

[1] B. J. Birch, *Cyclotomic fields and Kummer extensions*, in: *Algebraic Number Theory* (*Proc. Instructional Conf., Brighton*, 1965), Thompson, Washington, D.C., 1967, pp. 85–93.

[2] P. Erdös, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen 4 (1956), pp. 201–206.

[3] C. Hooley, *On Artin's Conjecture*, J. Reine Angew. Math. 225 (1967), pp. 209–220.

[4] H. W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. 42 (1977), pp. 201–224.

[5] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* $25\cdot 10^9$, Math. Comp. 35 (1980), pp. 1003–1026.

[6] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, Acta Arith. 17 (1970), pp. 161–168.

[7] J. W. Wrench, Jr., *Evaluation of Artin's constant and the twin-prime constant*, Math. Comp. 15 (1961), pp. 396–398.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
Urbana, Illinois, U.S.A.
Current address:
DEPARTMENT OF STATISTICS AND COMPUTER SCIENCE
UNIVERSITY OF GEORGIA
Athens, Georgia 30602, U.S.A.

Received on 8.11.1979
and in revised form on 30.5.1980 (1181)

ACTA ARITHMETICA
XLI (1982)

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

by

J. Wójcik (Warszawa)

I proved in [4] the following

Theorem A. *Let f be a polynomial with rational integral coefficients, irreducible, primitive, with a positive leading coefficient. Assume that f is different from x and is not a cyclotomic polynomial. There exists a positive integer $k_0 = k_0(f)$ such that for every positive integer k divisible by k_0 and for all positive integers D and r, where $(r, D) = 1$ and $r \equiv 1 \bmod (D, k)$ there exist infinitely many primes q satisfying the following condition: the congruence $f(x^k) \equiv 0 \bmod q$ is soluble, $q \equiv 1 \bmod k$, $q \equiv r \bmod D$. The Dirichlet density σ of this set of primes satisfies the inequality*

$$\frac{c(f)}{C(f)k\varphi([D,k])} \leqslant \sigma \leqslant \frac{n}{\varkappa}\,\frac{c(f)}{C(f)\varphi([D,k])},$$

where

$$\varkappa = \begin{cases} 1 & \text{if } f \text{ is not reciprocal,} \\ 2 & \text{if } f \text{ is reciprocal,} \end{cases} \qquad n \text{ is the degree of } f,$$

$c(f)$, $C(f)$ denote certain natural numbers depending on f.

The main aim of this paper is to prove a related theorem in the case of what we call a k-normal polynomial. Let K be an arbitrary field. A polynomial $f \in K[x]$ is called *weakly normal over* K if $K(a)$ is the splitting field of f for every root a of f (see [1]).

Let k be any positive integer. The polynomial $f \in K[x]$ is called *k-normal over K* if $f(x)$ is irreducible over K and $f(x^k)$ is weakly normal over $K(\zeta_k)$. Obviously the polynomial f is 1-normal if and only if it is normal. If the field K is fixed, we simply say that f is *k-normal.*

The definitions and notation are taken from [4]. In particular E_k is the group of rationals congruent to 1 mod k. We shall prove the following

Theorem. *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. Assume that f is k-normal. Let α be any root of it. We have*

(1) $$\alpha = \beta^{n_1}\gamma^{n_1}, \quad \text{where } n_1 = (k, c(f)),\ \beta \text{ is cyclotomic},\ \gamma \in \mathbf{Q}(\alpha).$$

Further, let K denote the maximal cyclotomic subfield of $\mathbf{Q}(\alpha)$. Let us put $K_1 = K(\beta)$. Let f_1 be the conductor of K_1. Let G_1 be a group of rationals mod f_1 *corresponding to K. Let us 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 satisfying the condition that $(D, r) = 1$ and the residue class* mod D *containing r contains a rational integer belonging to G_2 there exist infinitely many primes q satisfying the condition that $q \equiv r \bmod D$, $q \equiv 1 \bmod k$, and the congruence $f(x^k) \equiv 0 \bmod q$ is soluble in $x \in \mathbf{Z}$. The Dirichlet density of this set of primes is equal to*

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

Remark 1. In the case where the polynomial f and the positive integer k satisfy the assumptions of both Theorem A and the theorem given above we have

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

since $k \equiv 0 \bmod c(f)$, $k \equiv 0 \bmod f_1$ and $K_1 \subset P_{[D,k]}$ (see the beginning of the proof of Theorem A).

We shall use a standard lemma.

LEMMA 1. *Let K, L be subfields of some field. Let KL be algebraic over K. If $\alpha \in KL$ then $\alpha = a_1 b_1 + \ldots + a_m b_m$, where $a_j \in L$, $b_j \in K$.*

LEMMA 2. *Let K, L be subfields of some field. Assume that $L/K \cap L$ is a Galois extension and $\zeta_n \in L$. Let $\alpha \in K$. The equation*

(2) $$\alpha = \vartheta^n, \quad \vartheta \in KL,$$

has a solution in ϑ if and only if $\alpha = \beta^n\gamma^n$, $\beta \in L$, $\gamma \in K$.

Proof. The sufficiency of the condition is obvious. Assume that (2) holds. L is algebraic over $K \cap L$ and KL is algebraic over K. By Lemma 1

(3) $$\vartheta = \sum_{j=1}^{m} a_j b_j, \quad a_j \in L,\ b_j \in K,\ m \geqslant 1.$$

We may assume that $\vartheta \neq 0$ and m is minimal. It follows that $b_1, \ldots, b_m$ are linearly independent over L. By Theorem 4, p. 196 of [2] KL/K is a Galois extension. Let $\sigma \in G(KL)/K$. By (3) $\sigma(\vartheta) = \sum_{j=1}^{m} \sigma(a_j) b_j$. $\sigma(a_j) \in L$

since the extension $L/K \cap L$ is Galois. On the other hand, by (2) and (3)

$$\sigma(\vartheta) = \zeta_n^x \vartheta = \sum_{j=1}^{m} \zeta_n^x a_j b_j, \quad \zeta_n^x a_j \in L.$$

Comparing the coefficients of b_j, we have $\sigma(a_j) = \zeta_n^x a_j$. Since $\vartheta \neq 0$, we have $a_j \neq 0$ for a certain j. Hence $\sigma\left(\frac{\vartheta}{a_j}\right) = \frac{\vartheta}{a_j} \in K$ since σ was arbitrarily chosen. Hence $\vartheta = \beta\gamma$, $\beta = a_j \in L$, $\gamma \in K$ and $\alpha = \beta^n\gamma^n$.

Remark 2. The assertion of Lemma 2 does not hold if $\zeta_n \notin L$. We shall give the following example: $K = P_n$, $L = P_p$, p a prime, $p > 3$, $n | p-1$, $n > 2$.

Let χ be a character of degree n with conductor p. Let $\vartheta = \tau(\chi) = \sum_{x=1}^{p-1} \chi(x)\zeta_p^x$. It is well known that $\alpha = \vartheta^n = \tau^n(\chi) \in P_n = K$. Further, $\vartheta \in P_n P_p = KL$. The equality $\alpha = \beta^n\gamma^n$, $\beta \in L$, $\gamma \in K$ does not hold. Otherwise $\vartheta = \beta\gamma_1$, $\beta \in P_p$, $\gamma_1 \in P$ and $\vartheta = \gamma_1 \sum_{x=1}^{p-1} a_x \zeta_p^x$, $a_x \in \mathbf{Q}$.

The numbers $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ form a basis for the extensions $P_p/\mathbf{Q}$ and $P_n P_p/P_n$. Hence, comparing the coefficients of ζ_p^x, we have $\chi(x) = \gamma_1 a_x$. For $x = 1$ we have $\gamma_1 = 1/a_1 \in \mathbf{Q}$, $\chi(x) \in \mathbf{Q}$, $\chi(x) = \pm 1$ for $x = 1, \ldots, p-1$, which is impossible because $n > 2$.

LEMMA 3. *Let K be a field. Let $\alpha \in K$. The equation*

$$\alpha = \vartheta^n, \quad \vartheta \in K^{mc}$$

has a solution in ϑ if and only if $\alpha = \beta^n\gamma^n$, where β is cyclotomic and $\gamma \in K$.

Proof. The proof follows at once from Lemma 2 since $K^{mc} = KL$, where L is the field generated by all roots of unity.

LEMMA 4. *Let k_1 be a field of characteristic 0. Let L_1 be a cyclotomic field; K_1, K_2 denote maximal cyclotomic subfields of the fields k_1, $k_1 L_1$, respectively. Then $K_2 = K_1 L_1$.*

Proof (due to A. Schinzel). It is enough to prove that $K_2 \subset K_1 L_1$. Take an arbitrary element α of $K_2 = \mathbf{Q}^{mc} \cap k_1 L_1$. By Lemma 1 it is of the form

$$\sum_{i=1}^{j} a_i b_i, \quad \text{where } a_i \in k_1,\ b_i \in L_1.$$

Let $\mathbf{Q}(b_1, \ldots, b_j) = \mathbf{Q}(\vartheta) \subset L_1$. We get

(4) $$\alpha = \sum_{i=0}^{d-1} c_i \vartheta^i, \quad \text{where } c_1 \in k_1,\ d = (k_1(\vartheta) : k_1).$$

icm

Taking conjugates with respect to k_1 we obtain

$$\alpha^{(\nu)} = \sum_{i=0}^{d-1} c_i \vartheta^{(\nu)i} \quad (\nu = 1, \ldots, d).$$

From Cramer's formulae it follows that

$$c_i \in \boldsymbol{Q}(\alpha^{(1)}, \ldots, \alpha^{(d)};\ \vartheta^{(1)}, \ldots, \vartheta^{(d)}) \subset \boldsymbol{Q}^{mc}.$$

Hence $c_i \in \boldsymbol{Q}^{mc} \cap k_1 = K_1$ and we get from (4) $\alpha \in K_1 L_1$.

LEMMA 5. *Let F and m be positive integers. Let k_2 be a finite algebraic number field. Assume that $\beta \in k_2$, β is different from zero and from roots of unity, $\zeta_m \in k_2$ and $(c_{k_2}(\beta), m) = 1$. There exists an ideal $\mathfrak{a}$ of k_2 such that $\left(\frac{\beta}{\mathfrak{a}}\right)_m = \zeta_m$, $N\mathfrak{a} \equiv 1 \bmod F$, $(\mathfrak{a}, F) = 1$.*

Proof. We may suppose that F is divisible by all conductors of power residue symbols occurring in this proof. If the assertion of the lemma does not hold, then for some positive integer d such that $d \mid m$, $d < m$ we have: If $(\mathfrak{a}, F) = 1$ and $N\mathfrak{a} \equiv 1 \bmod F$ then $\left(\frac{\beta}{\mathfrak{a}}\right)_m = \zeta_d^x$ for a certain x depending on $\mathfrak{a}$. Hence $\left(\frac{\beta^d}{\mathfrak{a}}\right)_m = 1$ for $N\mathfrak{a} \equiv 1 \bmod F$, $(\mathfrak{a}, F) = 1$. Hence

$$\left(\frac{\beta^d \mid k_2 P_F}{\mathfrak{b}}\right)_m = \left(\frac{\beta^d \mid k_2}{N_{k_2 P_F / k_2} \mathfrak{b}}\right)_m = 1$$

for any ideal $\mathfrak{b}$ of $k_2 P_F$ prime to F since

$$N_{k_2/\boldsymbol{Q}}(N_{k_2 P_F/k_2} \mathfrak{b}) = N_{k_2 P_F/\boldsymbol{Q}} \mathfrak{b} \equiv 1 \bmod F.$$

This means that β^d is the mth power residue for almost all prime ideals of $k_2 P_F$ and by Theorem 16.7 (I) of [3], p. 153, $\beta^d = \gamma^m$, $\gamma \in k_2 P_F$. Hence $\beta = \gamma_1^{m_1}$, $\gamma_1 \in k_2^{mc}$, $m_1 = m/d > 1$. By Lemma 1 of [4] $c_{k_2}(\beta)$, $c_{k_2}(\gamma_1)$ are positive integers. By Lemma 6 of [4] $c_{k_2}(\beta) = m_1 c_{k_2}(\gamma_1)$. Thus $m_1 \mid c_{k_2}(\beta)$, $m_1 \mid m$, $m_1 > 1$, which is impossible since $(c_{k_2}(\beta), m) = 1$.

LEMMA 6. *Let F and m be positive integers. Let k_2 be a finite algebraic number field, $\beta \in k_2$, where β is different from zero and from roots of unity, $\zeta_m \in k_2$ and $(c_{k_2}(\beta), m) = 1$. Let G_2 be a group of rationals* mod F *corresponding to $k_2 \cap P_F$. For any rational integer x and $s \in G_2$ there exists an ideal $\mathfrak{a}$ of k_2 such that*

$$\left(\frac{\beta}{\mathfrak{a}}\right)_m = \zeta_m^x, \quad (\mathfrak{a}, F) = 1,\ N\mathfrak{a} \equiv s \bmod F.$$

Proof. We may suppose that F is divisible by $f(k_2(\sqrt[m]{\beta})/k_2)$. By Lemma 2 of [4] there exists an ideal $\mathfrak{a}_1$ of k_2 such that $s \equiv N\mathfrak{a}_1 \bmod F$, $(\mathfrak{a}_1, F) = 1$. By Lemma 5 there exists an ideal $\mathfrak{a}_2$ of k_2 such that $\left(\frac{\beta}{\mathfrak{a}_2}\right)_m = \zeta_m$, $(\mathfrak{a}_2, F) = 1$, $N\mathfrak{a}_2 \equiv 1 \bmod F$. Let $\left(\frac{\beta}{\mathfrak{a}_1}\right)_m = \zeta_m^a$. It is enough to take $\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2^{x-a}$.

Proof of the theorem. Let α be any root of the polynomial f. By the assumption α is different from zero and from roots of unity. Let us put $k_1 = \boldsymbol{Q}(\alpha)$. By Lemma 1 of [4] $c(f) = c_{k_1}(\alpha)$ is a positive integer. We have

(5) $$\alpha = \beta_1^{n_1}, \quad \beta_1 \in k_1^{mc},\ n_1 = (k, c(f)).$$

Let us put $m = k/n_1$. By Lemma 6 of [4]:

$$c(f) = c_{k_1}(\alpha) = n_1 c_{k_1}(\beta_1).$$

Hence

$$n_1 = (n_1 m, n_1 c_{k_1}(\beta_1)) = n_1(m, c_{k_1}(\beta_1)).$$

Thus

(6) $$(m, c_{k_1}(\beta_1)) = 1.$$

By Lemma 3 and (5) $\alpha = \beta^{n_1}\gamma^{n_1}$, $\beta \in \boldsymbol{Q}^{mc}$, $\gamma \in k_1$. Thus (1).

We may suppose that

(7) $$\beta_1 = \beta \cdot \gamma, \quad \beta \in \boldsymbol{Q}^{mc},\ \gamma \in k_1.$$

Let us put $k_2 = k_1 P_k(\beta)$, $\left(\frac{\gamma}{\mathfrak{a}}\right)_s = \left(\frac{\gamma \mid k_2}{\mathfrak{a}}\right)_s$ for $s \mid k$. We have $\alpha \in k_2$, $\beta_1 \in k_2$ and

(8) $$\left(\frac{\alpha}{\mathfrak{a}}\right)_k = \left(\frac{\beta_1}{\mathfrak{a}}\right)_m$$

by (5) and (7). By Lemma 4 the field $K \cdot P_k(\beta) = K(\beta) \cdot P_k = K_1 P_k$ is the maximal cyclotomic subfield of k_2. We have $K_1 P_k \subset P_{[k, f_1]}$.

Let us put $\bar{G}_1 = \{s\colon s \in \boldsymbol{Q},\ (s, [k, f_1]) = 1,\ s \in G_1\}$, $\bar{E}_k = \{s\colon s \in \boldsymbol{Q},\ (s, [k, f_1]) = 1,\ s \in E_k\}$, $\bar{G}_1$, $\bar{E}_k$ are groups of rationals mod $[k, f_1]$ corresponding to the fields K_1, P_k, respectively.

By the Galois theory $\bar{G}_1 \cap \bar{E}_k = G_1 \cap E_k = G_2$ is the group of rationals mod $[k, f_1]$ corresponding to the field $K_1 P_k$.

Let D be any positive integer. Let F be a positive integer divisible by $k f_1 D$ and by all conductors of power residue symbols occurring in this proof. Clearly $K_1 P_k \subset P_F$. Hence

$$k_2 \cap P_F = K_1 P_k,$$

since $K_1 P_k$ is the maximal cyclotomic subfield of k_2. Let us put

$$\bar{G}_2 = \{s\colon s \in \boldsymbol{Q},\ (s, F) = 1,\ s \in G_2\}.$$

$\bar{G}_2$ is the group of rationals mod F corresponding to $k_2 \cap P_F$. Put

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

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

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

By the assumption on F, A, H_1, H are groups of ideals mod F in virtue of Artin's reciprocity law. Let $r \in \bar{G}_2$. We have $k_2^{mc} = k_1^{mc}$. Hence $c_{k_2}(\beta_1) = c_{k_1}(\beta_1)$ and by (6)

$$(9) \qquad (c_{k_2}(\beta_1), m) = 1.$$

By Lemma 6 there exists an ideal $\mathfrak{a}_1$ of k_2 such that $(\mathfrak{a}_1, F) = 1$, $N\mathfrak{a}_1 \equiv r \bmod F$, $\left(\frac{\beta_1}{\mathfrak{a}_1}\right)_m = 1$. Let C denote the coset of A with respect to H containing $\mathfrak{a}_1$, i.e. by (8)

$$C = \left\{\mathfrak{a}\colon \mathfrak{a} \text{ an ideal of } k_2,\ (\mathfrak{a}, F) = 1,\ N\mathfrak{a} \equiv r \bmod F,\ \left(\frac{a}{\mathfrak{a}}\right)_k = 1\right\},$$
$$(r, F) = 1,\ r \in G_2.$$

We shall prove that G_2 is uniquely determined by the polynomial f and positive integer k. Let a' be any root of f. We have by (1) $a' = \beta'^{n_1}\gamma'^{n_1}$, $\beta' \in Q^{mc}$, $\gamma' \in Q(a')$. Let K' be the maximal cyclotomic subfield of $Q(a')$. We have

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

By Lemma 4 $K(\beta) = K \cdot Q(\beta)$ is the maximal cyclotomic subfield of the field $k_1 Q(\beta) = k_1(\beta) = k_1(\beta_1) = Q(\beta_1)$ by (5) and (7). Analogously $K'(\beta')$ is the maximal cyclotomic subfield of the field $Q(\beta_1')$. Let f_1' be the conductor of $K'(\beta')$. Clearly $a \in Q(\beta_1)$. Let τ be an isomorphism of $Q(\beta_1)$ such that $\tau(a) = a'$. We have $a' = \beta_2'^{n_1}$ where $\beta_2' = \tau(\beta_1)$ by (6). Hence $\beta_1' = \zeta_{n_1}^a \beta_2'$ and

$$(10) \qquad Q(\beta_1')P_k = Q(\zeta_{n_1}^a \beta_2')P_k = Q(\beta_2')P_k, \qquad (n_1 | k).$$

$K(\beta)$ is the maximal cyclotomic subfield of $Q(\beta_2')$ because $Q(\beta_2') = \tau Q(\beta_1)$. By (10) and by Lemma 4 $K'(\beta')P_k = K(\beta)P_k = K_1 P_k$. Since a', β' are chosen arbitrarily, the latter formula means that $K_1 P_k$ is uniquely determined by the polynomial f and by the positive integer k. The conductor of $K_1 P_k$ is equal to $[k, f_1]$ or to $[k/2, f_1]$ and $[k, f_1] = [k, f_1']$ is uniquely determined by k and f. As we have mentioned above, G_2 is the group of rationals mod$[k, f_1]$ corresponding to $K_1 P_k$. Hence G_2 is uniquely determined by k and f.

Let us put

$$B = \{q\colon q \text{ a prime},\ q \equiv r \bmod F, \text{ the congruence } f(x^k) \equiv 0 \bmod q \text{ is soluble}\},$$

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

We have

(i) If $f(x^k) \equiv 0 \bmod q$ $(x \in Z)$, $q \equiv 1 \bmod k$ and q is a sufficiently large prime number, then q splits completely in k_2, moreover if $q \in B$ then q is the product of $|k_2|$ prime ideals of degree one belonging to C.

Let us put $k_3 = P_k(\sqrt[k]{a})$. Obviously $a \in k_3$. Hence $k_1 \subset k_3$. Further $\beta_1 = \zeta_{n_1}^b (\sqrt[k]{a})^m$ by (6). Thus $\beta_1 \in k_3$. By (7) $\beta = \beta_1/\gamma \in k_3$. Hence $P_k \subset k_2 \subset k_3$. Let $\mathfrak{q}$ be a prime ideal of k_2 dividing q. Let $\bar{Q} | \mathfrak{q}$, $\bar{Q} | \mathfrak{Q}$ where $\bar{Q}$ is a prime ideal of k_3 and $\mathfrak{Q}$ is a prime ideal of P_k. We have

$$f(x^k) = a_0 \prod_{j=1}^{kn} (x - \xi_j) \equiv 0 \bmod \bar{Q},$$

where n is the degree of f, and a_0 its leading coefficient. Since f is k-normal, we get $k_3 = P_k(\xi_j) = Q(\xi_j, \zeta_k)$. In particular $\xi_j \in k_3$ $(j = 1, \ldots, kn)$. Hence $\xi_j \equiv x \bmod \bar{Q}$ for a certain j $(x \in Z)$, $\mathfrak{Q}$ is a prime ideal of degree one in P_k since $q \equiv 1 \bmod k$. Hence $\zeta_k \equiv y \bmod \mathfrak{Q}$ and also $\zeta_k \equiv y \bmod \bar{Q}$ $(y \in Z)$. Let $\omega_1, \ldots, \omega_t$, $t = |k_3|$ be an integral basis of k_3. We have $\omega_i = g_i(\xi_j, \zeta_k)$ with $g_i \in Q[x_1, x_2]$ $(i = 1, \ldots, t)$. Hence every integer of k_3 is congruent to a rational integer mod $\bar{Q}$. This means that $\bar{Q}$ is of degree one. Hence $\mathfrak{q}$ is of degree one. Since q is sufficiently large, we have $\sqrt[k]{a} \equiv z \bmod \bar{Q}$ $(z \in Z)$. Thus $a \equiv z^k \bmod \bar{Q}$, i.e. $a \equiv z^k \bmod \mathfrak{q}$ since $a \in k_2$. Thus $\left(\frac{a}{\mathfrak{q}}\right)_k = 1$. If additionally $q \in B$ then $q = N_{k_2/Q}\mathfrak{q} \equiv r \bmod F$ and $\mathfrak{q} \in C$. (i) follows at once since $\mathfrak{q}$ was chosen arbitrarily.

On the other hand, if $\mathfrak{q} \in C$ and $\mathfrak{q}$ is a prime ideal of degree one and a prime number $q = N\mathfrak{q}$ is sufficiently large, then $q \equiv r \bmod F$ and $x^k \equiv a \bmod \mathfrak{q}$ for a certain $x \in Z$. Hence $f(x^k) = (x^k - a)g(x) \equiv 0 \bmod \mathfrak{q}$ with $g(x) \in k_2[x]$ $(a \in k_2)$. Thus $f(x^k) \equiv 0 \bmod q$. This means that $q \in B$. Let us put

$$(11) \qquad h = (A : H).$$

Hence by (i) and by Hecke's theorem

$$\frac{1}{h} = d(C) = \lim_{s \to 1+0} \frac{\sum_{\mathfrak{q} \in C} 1/(N\mathfrak{q})^s}{\log(1/(s-1))} = |k_2| \lim_{s \to 1+0} \frac{\sum_{q \in B} 1/q^s}{\log(1/(s-1))} = |k_2|\, d(B),$$

where $\mathfrak{q}$ are prime ideals of degree one. Hence $d(B) = 1/h|k_2|$. By Lemma 2 of [4] the quotient group A/H_1 is isomorphic with $\bar{G}_2/E_F$ since $\bar{G}_2$ is a group of rationals mod F corresponding to $k_2 \cap P_F$. By the Galois theory

$$(A:H_1) = (\bar{G}_2 : E_F) = (P_F : k_2 \cap P_F)$$
$$= (P_F : K_1 P_k) = |P_F|/|K_1 P_k| = \varphi(F)/|K_1 P_k|.$$

By (8), (9) and Lemma 6 ($s = 1$):

$$(H_1 : H) = m = k/(k, c(f)).$$

By (11)

$$h = (A:H) = (A:H_1)(H_1:H) = \big(\varphi(F)/|K_1P_k|\big)\cdot\big(k/(k, c(f))\big).$$

Hence

$$d(B) = \frac{(k, c(f))}{k\varphi(F)}\,\frac{|K_1P_k|}{|k_2|}.$$

We have $k_2 = k_1P_k(\beta) = k_1P_k\cdot K(\beta) = k_1K_1P_k$. Hence

$$\frac{|k_2|}{|K_1P_k|} = \frac{|k_1K_1P_k|}{|K_1P_k|} = \frac{|k_1|}{|k_1\cap K_1P_k|} = \frac{|k_1|}{|K|} = \frac{n}{|K|} = C(f)$$

since K_1P_k is the maximal cyclotomic subfield of k_2 and $k_1 \cap K_1P_k = K$. Hence

$$d(B) = \frac{(k, c(f))}{C(f)k\varphi(F)}. \tag{12}$$

Assume first that $D \equiv 0 \bmod [k, f_1]$. Let us put

$$B' = \{q\colon\ q \text{ a prime number, } q \equiv r \bmod D, \text{ the congruence } f(x^k) \equiv 0 \bmod q \text{ is soluble}\},$$

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

We have $D|F$. Let P be the group of all residue classes mod F prime to F and P_1 the subgroup of residue classes mod F congruent to 1 mod D. Since for each rational integer ξ prime to D there exists a rational integer η prime to F such that $\eta \equiv \xi \bmod D$, we have $(P:P_1) = \varphi(D)$. Hence the number of residue classes mod F which are congruent to r mod D is equal to $\varphi(F)/\varphi(D)$ and all these classes are contained in G_2 since D is divisible by k and by f_1. It follows that B' apart from at most finitely many prime numbers q dividing F is the set theoretic-union of $\varphi(F)/\varphi(D)$ disjoint sets of type B. Since by (12) the Dirichlet density of these sets does not depend on r we have

$$d(B') = \frac{\varphi(F)}{\varphi(D)}\,d(B)$$

and

$$d(B') = \frac{(k, c(f))}{C(f)k\varphi(D)}. \tag{13}$$

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

$$G_1 = r_1E_{f_1} \cup r_2E_{f_1} \cup \ldots \cup r_tE_{f_1}, \quad t = (G_1 : E_{f_1}).$$

Let D be any positive integer. Put

$$B_j = \{q\colon\ q \text{ a prime, } q \equiv r \bmod D,\ q \equiv 1 \bmod k,\ q \equiv r_j \bmod f_1, \text{ the congruence } f(x^k) \equiv 0 \bmod q \text{ is soluble}\},$$

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

$$r_j' \equiv \begin{cases} r \bmod D, \\ 1 \bmod k, \\ r_j \bmod f_1. \end{cases} \tag{14}$$

Obviously

$$B_j = \{q\colon\ q \text{ a prime, } q \equiv r_j' \bmod [D, k, f_1], \text{ the congruence } f(x^k) \equiv 0 \bmod q \text{ is soluble}\},$$

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

By (13) (the theorem for $D \equiv 0 \bmod [k, f_1]$)

$$d(B_j) = \frac{(k, c(f))}{C(f)k\varphi([D, k, f_1])}. \tag{15}$$

Let us put

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

where $(r, D) = 1$ and the residue class mod D containing r contains also a number belonging to G_2.

There exists a rational integer r' such that

$$r' \equiv \begin{cases} r \bmod D, \\ 1 \bmod k, \end{cases} \quad r' \in G_1. \tag{16}$$

We have

$$B'' = \{q\colon\ q \text{ a prime, } q \equiv r' \bmod [D, k], \text{ the congruence } f(x^k) \equiv 0 \bmod q \text{ is soluble}\}.$$

We have $B_j \subset B''$. Let $q \in B''$ and let q be sufficiently large. By (i) q splits completely in k_2 and also in K_1. Further $K_1 \subset P_{f_1}$. By Lemma 2 of [4] $q \in G_1$. There exists an index j such that $q \equiv r_j \bmod f_1$. Thus $q \in B_j$ (as r'_j we may take q). Hence B'' apart from at most finitely many numbers is the set-theoretic union of N_1 disjoint sets of type B_j, where N_1 is the number of those j from the sequence $1, 2, \ldots, t$ for which there exists an r'_j satisfying (14). By (16) N_1 is the number of those j for which there exists an r'_j satisfying the condition

$$r'_j \equiv \begin{cases} r' \bmod [D, k], \\ r_j \bmod f_1. \end{cases} \tag{17}$$

By (15) $d(B_j)$ does not depend on j. Hence

$$d(B'') = N_1 d(B_j). \tag{18}$$

Let us put

$$\bar{\bar{G}}_1 = \{s\colon s \in Q,\ (s, [D, k, f_1]) = 1,\ s \in G_1\}.$$

$\bar{\bar{G}}_1$ is the group of rationals mod $[D, k, f_1]$ corresponding to K_1. By (17) N_1 is the number of residue classes mod $[D, k, f_1]$ which are contained in $\bar{\bar{G}}_1$ and are congruent to r' mod $[D, k]$. Since $r' \in \bar{\bar{G}}_1$ we have

$$N_1 = |r' E_{[D,k,f_1]}(\bar{\bar{G}}_1 \cap E_{[D,k]}/E_{[D,k,f_1]})| = |\bar{\bar{G}}_1 \cap E_{[D,k]}/E_{[D,k,f_1]}|.$$

By the Galois theory

$$N_1 = (P_{[D,k,f_1]}\colon K_1 P_{[D,k]}) = \frac{|P_{[D,k,f_1]}|}{|K_1 P_{[D,k]}|} = \frac{|P_{[D,k,f_1]}|}{|P_{[D,k]}|}\,\frac{|K_1 \cap P_{[D,k]}|}{|K_1|}$$
$$= \frac{\varphi([D, k, f_1])}{\varphi([D, k])}\,\frac{|K_1 \cap P_{[D,k]}|}{|K_1|}.$$

Hence by (18) and (15)

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

The theorem is proved.

Remark 3. We have also shown in the last part of the proof that if $q \in B''$ and q is sufficiently large then $q \in G_1$. Since $q \equiv 1 \bmod k$, it follows that $q \in G_2$. The existence of a number belonging to G_2 in the residue class mod D containing r is the necessary condition for the existence of infinitely many prime numbers with the property mentioned in the theorem. In proving that G_2 is uniquely determined by k and f we did not use the fact that f is k-normal.

References

[1] D. Gay, *On normal radical extensions of real fields*, Acta Arith. 35 (1979), pp. 271–298.
[2] S. Lang, *Algebra*, Reading Mass. 1965.
[3] Henry B. Mann, *Introduction to algebraic number theory*, Columbus 1955.
[4] J. Wójcik, *Contributions to the theory of Kummer extensions*, Acta Arith. 40 (1982), pp. 155–174.

Received on 20. 12. 1979
and in revised form on 10. 5. 1980 (1190)