Štefan Schwarz

On the reducibility of binomial congruences and on the bound of the least integer belonging to a given exponent $\mod p$

Časopis pro pěstování matematiky a fysiky, Vol. 74 (1949), No. 1, 1--16

Persistent URL: http://dml.cz/dmlcz/109143

Časopis pro pěstování matematiky a fysiky, roč. 74 (1949)

ON THE REDUCIBILITY OF BINOMIAL CONGRUENCES AND ON THE BOUND OF THE LEAST INTEGER BELONGING TO A GIVEN EXPONENT mod$p$

ŠTEFAN SCHWARZ, Bratislava.

(Received February 28, 1948.)

Let

$$x^n - a \equiv 0 \;(\text{mod} p), \quad (n, p) = (a, p) = 1, \tag{1}$$

be a congruence of degree $n \geqq 1$. Let k be an integer, $1 \leqq k \leqq n$. Let $\sigma_k = \sigma_k(a)$ denote the number of irreducible factors of degree k of the congruence (1).

In a paper[1]) published in czech language I found a system of recurrent relations, which enable us to calculate the numbers $\sigma_1, \sigma_2, \ldots, \sigma_n$ (mod$p$) (except the cases $k \equiv 0$ (mod$p$)).

In this paper — which may be read without reference to the former investigations — we give essentially preciser results by finding explicit formulae for the numbers $\sigma_k(a)$.

The method of our investigation is elementary and it is rather suprising that I did not found the explicit form of Theorem 1 in the literature, though it deals with a question entirely classical.[2])

In section I we prove the fundamental Theorem 1 giving the formula for the number $\sigma_k(a)$.

In section II we give several easy but interesting applications. Some of them are known (with other proofs) and useful in the theory of cyclotomic fields.

In section III we give another form to the results obtained in section I by introducing the theory of characters.

In section IV we use the formula (13) to generalize a result due to I. M. VINOGRADOV. Let $g = g(p)$ be the least primitive root mod$p$. VINOGRADOV[3]) proved $g(p) = O(p^{\frac{1}{2}+\varepsilon})$. We shall show: Let l be an integer;

[1]) Časopis pro pěst. mat. fys., **71** (1945), p. 21—31.

[2]) E. g., in L. A. DICKSON'S History of the Theory of Numbers I, Washington, 1934, there are 41 pages devoted to related questions (p. 181—222).

[3]) See E. LANDAU, Vorlesungen über Zahlentheorie II, 1927, p. 180.

$l/p - 1$. Let $g = g(p, l)$ be the least integer belonging to the exponent l (mod$p$). Then it is $g(p, l) = O(l^{\varepsilon-1}p^{\frac{3}{2}})$ for every positive ε. Hence, for $l = p - 1$ we have the result of VINOGRADOV.[4])

In section V we generalize the results by considering binomial polynomials over an arbitrary finite field as ground field. As an application of the results obtained we prove Theorem 8, which is a generalization of a theorem due to H. DAVENPORT.[5])

I.

Theorem I. *Let* (1) *be a congruence of degree $n \geqq 1$, p a prime. Let t be an integer, $1 \leqq t \leqq n$. Put $d_t = (n, p^t - 1)$. Let σ_k denote the number of irreducible factors of degree k of the congruence* (1). *Let $\mu(t)$ be the* MÖBIUS *function. Let δ_t be defined as follows:*

$$\delta_t = \begin{cases} 0 \text{ if } a^{\frac{p^t-1}{d_t}} \not\equiv 1 \pmod{p}, \\ d_t \text{ if } a^{\frac{p^t-1}{d_t}} \equiv 1 \pmod{p}. \end{cases}$$

Then it holds

$$\sigma_k = \frac{1}{k}\sum_{t|k}\mu\left(\frac{k}{t}\right)\delta_t, \tag{1a}$$

where t runs through all divisors of k.

We need the following simple

Lemma I. *Let $s \geqq 1$, $n \geqq 1$ be two integers. Let $GF(p^s)$ be a* GALOIS *field. Let $\alpha \neq 0$ be an arbitrary element, $\alpha \in GF(p^s)$. Let us denote $d_s = (n, p^s - 1)$. Then the equation*

$$\xi^n - \alpha = 0 \tag{2}$$

has solutions with $\xi \in GF(p^s)$ if and only if[6])

$$\alpha^{\frac{p^s-1}{d_s}} = 1. \tag{3}$$

The condition (3) *being satisfied, the equation* (2) *has exactly d_s (different) solutions in $GF(p^s)$.*

Proof. It is well-known: the multiplicative group of the field $GF(p^s)$ is cyclic. That is: there exists an element $g \in GF(p^s)$ such that the sequence

$$g, g^2, g^3, \ldots, g^{p^s-1} = 1$$

represents just all non-zero elements of the field $GF(p^s)$.

[4]) The constant implied by the symbol O depends only on ε.

[5]) H. DAVENPORT, Quaterly Journal of Math., **8** (1937), p. 308—312.

[6]) 1 denotes the unity element of the field $GF(p^s)$.

Let $\alpha = g^b$, $\xi = g^x$ $(1 \leqq b \leqq p^s - 1,\ 1 \leqq x \leqq p^s - 1)$. The equation (2) will be satisfied if and only if

$$xn - b \equiv 0 \ (\mathrm{mod} p^s - 1). \tag{3a}$$

Let us denote $\frac{p^s - 1}{d_s} = m$.

i) Let be $d_s \nmid b$. Then (3a) — and therefore (2) — have not solutions. In this case it is certainly $\alpha^m = g^{bm} \not\equiv 1$ since the exponent is not divisible by $p^s - 1$. Conversely, if $\alpha^m \not\equiv 1$, the number bm is not divisible by $p^s - 1$, i. e. $d_s \nmid b$. The relations (3a) and (2) have not solutions.

ii) Let be d_s/b. The congruence (3a) has just d_s (incongruent) solutions, namely $x_0 + i \,.\, m$ $(i = 0, 1, \ldots, d_s - 1)$, where x_0 is the unique solutions of

$$\frac{n}{d_s} x - \frac{b}{d_s} \equiv 0 \ (\mathrm{mod} m).$$

The equation (2) has in $G\,F(p^s)$ just d_s different solutions: $\xi = g^{x_0 + i.m}$ $(i = 0, 1, 2, \ldots, d_s - 1)$. Since the exponent bm is a multiple of $p^s - 1$ there holds $\alpha^m = g^{bm} = 1$. Conversely, if $g^{bm} = 1$ it is d_s/b; the relations (2) and (3a) have just d_s solutions. This proves our Lemma.

Proof of Theorem I. Let us consider the congruence (1) as an equation in $G\,F(p)$, field of residue-classes (mod$p$). Let k be a positive integer. Let $k' > k'' > k''' > \ldots > 1$ be all divisors of k less then k. Let $\varphi(x)$ be an irreducible polynomial of the field $G\,F(p)$ of degree k. Let j be one root of $\varphi(x) = 0$. Then all roots of all irreducible equations $\epsilon\, GF(p)$ of degrees $k, k', k'', \ldots, 1$ are in the field $G\,F(p)[j] = G\,F(p^k)$.

Let the polynomial $x^n - a$, $a \in G\,F(p)$ have σ_k irreducible factors of degree k, $\sigma_{k'}$ irreducible factors of degree k', ..., σ_1 linear factors. Then the equation $x^n - a = 0$ has just

$$k\sigma_k + k'\sigma_{k'} + \ldots + \sigma_1$$

solutions in $G\,F(p^k)$.

Now we use Lemma 1.

i) If

$$a^{\frac{p^k - 1}{d_k}} \equiv 1 \ (\mathrm{mod} p)$$

the number of solutions of $x^n - a = 0$ in the field $G\,F(p^k)$ is just d_k. In this case it must hold therefore

$$k\sigma_k + k'\sigma_{k'} + \ldots + \sigma_1 = d_k. \tag{4}$$

ii) If

$$a^{\frac{p^k - 1}{d_k}} \not\equiv 1 \ (\mathrm{mod} p)$$

the number of solutions is equal to zero. Comparing the results, we obtain again

$$k\sigma_k + k'\sigma_{k'} + \dots + \sigma_1 = 0. \tag{5}$$

By introducing the symbol δ_k defined above, we can write (4) and (5) in the common form

$$k\sigma_k + k'\sigma_{k'} + \dots + \sigma_1 = \delta_k,$$

$$\sum_{t/k} t\sigma_t = \delta_k. \tag{6}$$

We write the equation (6) for $k = 1, 2, 3, \dots$ Using the Möbius formula for inversion, we get

$$k\sigma_k = \sum_{t/k} \mu\left(\frac{k}{t}\right) \delta_t.$$

This proves Theorem 1.

II.

We shall apply the result of Theorem 1 to some special congruences.

Theorem 2. *Let a belong* mod$p$ *to the exponent l. Then the polynomial $x^{p-1} - a$ is* (mod$p$) *equal to a product of $\frac{p-1}{l}$ irreducible polynomials of degree l.*

Proof. Since $d_t = (p-1, p^t - 1) = p - 1$, we have

$$\frac{p^t - 1}{d_t} = \frac{p^t - 1}{p - 1} = p^{t-1} + p^{t-2} + \dots + 1 \equiv t \pmod{p - 1}.$$

Therefore

$$\delta_t = \begin{cases} 0 & \text{if } a^t \not\equiv 1 \pmod{p}, \\ p - 1 & \text{if } a^t \equiv 1 \pmod{p}. \end{cases}$$

Since l is the least value of t for which $a^t \equiv 1 \pmod{p}$

$$\delta_t = \begin{cases} p - 1 \text{ if } t = l, 2l, \dots, \frac{p-1}{l} \, . \, l, \\ 0 \text{ otherwise.} \end{cases}$$

By Theorem 1

$$\sigma_k = \frac{p-1}{k} \sum_{t/k}{}' \mu\left(\frac{k}{t}\right), \tag{7}$$

where Σ' denotes that t runs through those of the divisors of k which are contained among the numbers $t = l, 2l, \dots, \frac{p-1}{l} \, . \, l$.

a) If $l \nmid k$, the sum in (7) is empty. Therefore $\sigma_k = 0$.

b) If l/k, the formula (7) can be written in the form

$$\sigma_k = \frac{p-1}{k} \sum_{t/\frac{k}{l}} \mu\left(\frac{\frac{k}{l}}{t}\right).$$

For $\frac{k}{l} > 1$, $\sigma_k = 0$. For $k = l$, $\sigma_k = \frac{p-1}{l}$.[7] This proves Theorem 2.

Theorem 3. *Let p, q be two different primes. Let p belong* mod$q$ *to the exponent l. Then the polynomial*

$$x^q - a, \quad (a, p) = 1, \tag{8}$$

is decomposible (mod$p$) *in the following manner:*

i) *If $l = 1$ and $a^{\frac{p-1}{q}} \equiv 1$* (mod$p$), *the polynomial* (8) *splits in q different factors.*

ii) *If $l = 1$ and $a^{\frac{p-1}{q}} \not\equiv 1$* (mod$p$), *the polynomial* (8) *is irreducible.*

iii) *If $l > 1$, the polynomial* (8) *is a product of one linear and $\frac{q-1}{l}$ irreducible polynomials of degree l.*

Proof.[8] i) By supposition $q/p-1$, therefore $d_t = (q, p^t - 1) = q$ for every t.

It is further

$$a^{\frac{p^t-1}{d_t}} = a^{\frac{p-1}{q}(1+p+\ldots+p^{t-1})} \equiv a^{\frac{p-1}{q}.t} \ (\text{mod} p). \tag{9}$$

Since $a^{\frac{p-1}{q}} \equiv 1$ (mod$p$) we have also $a^{\frac{p^t-1}{d_t}} \equiv 1$, i. e. $\delta_t = q$ for every t.

$$\sigma_k = \begin{cases} \mu(1) \,.\, q = q & \text{for } k = 1, \\ \frac{q}{k} \sum_{t/k} \mu\left(\frac{k}{t}\right) = 0 & \text{for } k > 1. \end{cases}$$

ii) If $a^{\frac{p-1}{q}} \not\equiv 1$ (mod$p$) the relation (9) shows that $a^{\frac{p^t-1}{d_t}} \equiv 1$ (mod$p$) if and only if $t = q$. I. e. $\delta_1 = \delta_2 = \ldots = \delta_{q-1} = 0$, $\delta_q = q$.

$$\sigma_k = \begin{cases} \frac{1}{k} \sum_{t/k} \mu\left(\frac{k}{t}\right) . \, 0 = 0 & \text{for } 1 \leqq k < q; \\ \frac{1}{q} \sum_{t/q} \mu\left(\frac{q}{t}\right) \delta_t = \frac{1}{q} \mu(1) \, q = 1 & \text{for } k = q. \end{cases}$$

[7] We use the well known property of the MÖBIUS function: $\sum_{t/k} \mu(t) = 0$ if $k > 1$, $= 1$ if $k = 1$.

[8] This theorem is clearly of greatest importance in connection with the determination of prime ideal decompositions in KUMMER fields.

iii) If $l > 1$, then $d_1 = d_2 = \ldots = d_{l-1} = 1$, $d_l = q$. For $t = 1$, $2, \ldots, l - 1$ we have obviously $a^{\frac{p^t-1}{d_t}} \equiv 1 \pmod{p}$. For $t = l$ we conclude: since $q \nmid p - 1$ the integer $\frac{p^l - 1}{q}$ is divisible by $p - 1$ and $a^{\frac{p^l-1}{q}} = a^{\frac{p^l-1}{d_l}} \equiv 1 \pmod{p}$. Therefore $\delta_1 = \delta_2 = \ldots = \delta_{l-1} = 1$, $\delta_l = q$.

$$\sigma_k = \begin{cases} \delta_1 = 1 & \text{for } k = 1, \\ \frac{1}{k} \sum\limits_{t/k} \mu\left(\frac{k}{t}\right) . 1 = 0 & \text{for } 1 < k < l, \\ \frac{1}{l} \sum\limits_{t/l} \mu\left(\frac{l}{t}\right) \delta_t = \frac{1}{l} \left\{ \sum\limits_{t/l t \neq l} \mu\left(\frac{l}{t}\right) . 1 + \delta_l \right\} = \\ = \frac{1}{l}(-\mu(1) + q) = \frac{q-1}{l} & \text{for } k = l. \end{cases}$$

Theorem 3 is completely proved.

The result (1a) enables us to give a great number of other simple formulae. We restrict ourselves to quote the following two Theorems 4 and 5.

Theorem 4. *The number of irreducible factors of degree k of the polynomial $x^n - 1 \pmod{p}$ is given by the formula*

$$\sigma_k = \frac{1}{k} \sum_{t/k} \mu\left(\frac{k}{t}\right) . (n, p^t - 1). \tag{10}$$

Proof: Follows from (1a) if we pose $d_t = \delta_t$ for every t.

Remark. We can use the result of this and similar theorems to deduce some identities concerning the MÖBIUS function. One of them is the following.

Corollary. *Let k, n be positive integers, $1 < n \leqq k$, p a prime. Then it holds* $\sum\limits_{t/k} \mu\left(\frac{k}{t}\right) . (n, p^t - 1) = 0.$

Proof. Since $x^n - 1$ is reducible with respect to every modul p we have in (10) $\sigma_k = 0$ for all $k \geqq n$.

Theorem 5. *Let $F_n(x)$ be the cyclotomic polynomial of degree $\varphi(n)$.*[9] *Let $(n, p) = 1$. Then the number of irreducible factors* $\pmod{p}$ *of degree k of the polynomial $F_n(x)$ is given by the formula*

$$\sigma_k = \frac{1}{k} \sum_{t/k} \sum_{s/n} \mu\left(\frac{k}{t}\right) \mu\left(\frac{n}{s}\right) . (s, p^t - 1). \tag{11}$$

[9] Here and in the following $\varphi(n)$ is the EULER function. The coefficient of the highest power of $F_n(x)$ let be 1.

Proof. The polynomial $F_n(x)$ can be written in the form

$$F_n(x) = \prod_{s/n} (x^s - 1)^{\mu\left(\frac{n}{s}\right)}.$$

According to the formula (10) the number of irreducible factors (mod$p$) of degree k of the polynomial $x^s - 1$ is exactly

$$\frac{1}{k} \sum_{t/k} \mu\left(\frac{k}{t}\right) \cdot (s, p^t - 1).$$

Summing through all divisors s of n with the proper „multiplicity", we obtain the formula (11).

Remark. It is easy to transform the result (11) to another form which is used in the theory of cyclotomic fields:

Let p belong mod$n$ *to the exponent l. Then*

$$\sigma_k = \begin{cases} 0 & \text{if } k \neq l. \\ \frac{1}{l} \varphi(n) & \text{if } k = l. \end{cases}$$

Proof. Let $n = q_1^{v_1} \ldots q_r^{v_r}$ be the decomposition of n into prime factors. Then

$$\sum_{s/n} \mu\left(\frac{n}{s}\right) (s, p^t - 1) = \prod_{i=1}^{r} \sum_{s_i/q_i^{v_i}} \mu\left(\frac{q_i^{v_i}}{s_i}\right) (s_i, p^t - 1) =$$

$$= \prod_{i=1}^{r} \left\{ (q_i^{v_i}, p^t - 1) - (q_i^{v_i - 1}, p^t - 1) \right\},$$

$$\sigma_k = \frac{1}{k} \sum_{t/k} \mu\left(\frac{k}{t}\right) \prod_{i=1}^{r} \left\{ (q_i^{v_i}, p^t - 1) - (q_i^{v_i - 1}, p^t - 1) \right\}. \qquad (*)$$

The difference $(q_i^{v_i}, p^t - 1) - (q_i^{v_i - 1}, p^t - 1)$ is equal to zero or $q_i^{v_i} - q_i^{v_i - 1}$ according as $q_i^{v_i} \nmid p^p - 1$ or $q_i^{v_i} \mid p^t - 1$ holds.

Let l be the least value of t for which $q_i^{v_i} \mid p^t - 1$ for every i holds, i. e. the least value of t for which $n \mid p^t - 1$ holds. Then for every $k < l$ we have $\sigma_k = 0$. For $k = l$ there exists in (*) one and only one member $t = l$ different from zero. It is therefore

$$\sigma_l = \frac{1}{l} \prod_{i=1}^{r} (q_i^{v_i} - q_i^{v_i - 1}) = \frac{1}{l} \cdot \varphi(n), \text{ q. e. d.}$$

III.

One may express the results obtained in the formula (1a) in another form by introducing the characters of the multiplicative group $\mathfrak{G}^{(t)}$ of the field $G\,F(p^t)$.

$\mathfrak{G}^{(t)}$ is cyclic of order $p^t - 1$. There exist exactly $p^t - 1$ different characters of $\mathfrak{G}^{(t)}$. The principal character of $\mathfrak{G}^{(t)}$ let be $\chi_0^{(t)}$.

We prove first

Lemma 2. *Let $\mathfrak{G}^{(t)}$ be the multiplicative group of the field $G\,F(p^t)$. There exist, among the $p^t - 1$ characters of the qroup $\mathfrak{G}^{(t)}$, exactly $d_t = (n, p^t - 1)$ characters $\chi_j^{(t)}$ $(j = 0, 1, 2, \ldots, d_t - 1)$ for which the relation*

$$(\chi_j^{(t)})^n = \chi_0^{(t)}$$

holds.

Proof. Let g be a generating element of the group $\mathfrak{G}^{(t)}$. Every character $\chi^{(t)}$ is uniquely determined by the value of $\chi^{(t)}(g)$. The number $\chi^{(t)}(g)$ is a $(p^t - 1)$th root of unity. It is therefore of the form

$$\chi^{(t)}(g) = e^{\frac{2\pi i}{p^t-1}\cdot b}, \quad 0 \leqq b < p^t - 1.$$

The relation $(\chi^{(t)})^n = \chi_0^{(t)}$ implies $e^{\frac{2\pi i}{p^t-1}\cdot bn} = 1$, i. e. $p^t - 1/bn$. Putting $d_t = (n, p^t - 1)$ we have $\frac{p^t-1}{d_t} \Big/ \frac{n}{d_t}\, b$, i. e. $\frac{p-1}{d_t} \Big/ b$. Therefore

$$b = j \cdot \frac{p^t - 1}{d_t} \quad (j = 0, 1, 2, \ldots, d_t - 1).$$

Hence, we have exactly d_t characters defined by the property

$$\chi_j^{(t)}(g) = e^{\frac{2\pi i}{d_t}\cdot j} \quad (j = 0, 1, 2, \ldots, d_t - 1).$$

This proves Lemma 2.

Lemma 3. *Let $\chi_j^{(t)}$ $(j = 0, 1, 2, \ldots, d_t - 1)$ run through all d_t characters of Lemma 2. Then the number of solutions of*

$$x^n - a = 0, \; a \in G\,F(p^t); \; a \neq 0 \tag{12}$$

in the field $G\,F(p^t)$ is equal to the integer

$$\delta_t = \sum_{j=0}^{d_t-1} \chi_j^{(t)}(a).$$

Proof. Let g have the meaning of Lemma 2. Let $a = g^b$. We know (see the proof of Lemma 1): If $d_t \not/ b$ (12) has no solutions with $x \in G\,F(p^t)$; if d_t/b there exist exactly d_t such solutions.

On the other hand let us calculate

$$\sum_{j=0}^{d_t-1} \chi_j^{(t)}(a) = \sum_{j=0}^{d_t-1} \chi_j^{(t)}(g^b) = \sum_{j=0}^{d_t-1} [\chi_j^{(t)}(g)]^b =$$

$$= \sum_{j=0}^{d_t-1} e^{\frac{2\pi i}{d_t}.j.b} = \begin{cases} 0 \text{ if } d_t \nmid b, \\ d_t \text{ if } d_t / b. \end{cases}$$

This proves Lemma 3.

Using the results of Theorem 1, Lemma 2 and 3, we have:

Theorem 6. *Let the characters $\chi_j^{(t)}$ have the meaning from Lemma 2. Then the number of irreducible factors of degree k of the congruence* (1) *is given by the formula*

$$\sigma_k(a) = \frac{1}{k} \sum_{t/k} \mu\left(\frac{k}{t}\right) \sum_{j=0}^{d_t-1} \chi_j^{(t)}(a). \tag{13}$$

IV.

The result of Lemma 3 is valid if a is any non-zero element of $G\,F(p^t)$. In the following we shall suppose that a is moreover an element of the subfield $G\,F(p) \subset G\,F(p^t)$. Let us study therefore the values of the characters $\chi_j^{(t)}$ in the subgroup $\mathfrak{G}^{(1)}$, that is, in the multiplicative group of $G\,F(p)$.

We can represent all non-zero elements of the field $G\,F(p)$ by means of the generating element g of the group $\mathfrak{G}^{(t)}$ in the form

$$g^{\frac{p^t-1}{p-1}}, g^{2.\frac{p^t-1}{p-1}}, \ldots, g^{(p-1)\frac{p^t-1}{p-1}} = 1.$$

The element $\gamma = g^{\frac{p^t-1}{p-1}}$ is a generating element of the cyclic group $\mathfrak{G}^{(1)}$. A character χ of the group $\mathfrak{G}^{(1)}$ is uniquely given if we know the value $\chi(\gamma)$.

Our d_t characters of the group $\mathfrak{G}^{(t)}$ defined in Lemma 2 induce in the subgroup $\mathfrak{G}^{(1)}$ characters of the group $\mathfrak{G}^{(1)}$. Every such character is naturally a $(p-1)$th root of unity. It is namely

$$\chi_j^{(t)}(\gamma) = e^{2\pi i.\frac{j}{d_t}.\frac{p^t-1}{p-1}} = \varepsilon^{j\frac{p^t-1}{d_t}}, \tag{14}$$

where

$$\varepsilon = e^{\frac{2\pi i}{p-1}}.$$

The d_t different characters of the group $\mathfrak{G}^{(t)}$ induce in $\mathfrak{G}^{(1)}$ d_t characters which (considered as characters of $\mathfrak{G}^{(1)}$) must not be all different. Especially, there exists one and only one principal character $\chi_0^{(t)}$ of $\mathfrak{G}^{(t)}$, but among the d_t characters induced in $\mathfrak{G}^{(1)}$ there can exist several principal characters $\chi_0^{(1)}$ of $\mathfrak{G}^{(1)}$.

We prove

Lemma 4. *The number of principal characters of $\mathfrak{G}^{(1)}$ induced in $\mathfrak{G}^{(1)}$ by the d_t characters of $\mathfrak{G}^{(t)}$ mentioned in Lemma 2 is equal to the number of integers divisible by $p - 1$ in the sequence*

$$0, \frac{p^t - 1}{d_t}, 2 \cdot \frac{p^t - 1}{d_t}, \ldots, (d_t - 1) \frac{p^t - 1}{d_t}. \tag{15}$$

Proof. According to (14) our d_t characters applied to elements of $\mathfrak{G}^{(1)}$ give the table

$$\begin{array}{c|cccc}
 & \gamma, & \gamma^2, & \ldots, & \gamma^{p-1} = 1 \\
\hline
\chi_0^{(t)} & 1 & 1 & \ldots, & 1, \\
\chi_1^{(t)} & \varepsilon^{\frac{p^t-1}{d_t}}, & \varepsilon^{2\frac{p^t-1}{d_t}}, & \ldots, & 1, \\
\vdots & \vdots & \vdots & & \vdots \\
\chi_{d_t-1}^{(t)} & \varepsilon^{(d_t-1)\frac{p^t-1}{d_t}}, & \varepsilon^{2(d_t-1)\frac{p^t-1}{d_t}}, & \ldots, & 1.
\end{array}$$

Those and only those of these characters are principal characters of $\mathfrak{G}^{(1)}$ for which $\chi_j^{(t)}(\gamma) = 1$ holds. That are those for which $j \frac{p^t - 1}{d_t}$ is divisible by $p - 1$. This proves Lemma 4.

Theorem 7. *Let be $l/p - 1$. Let $g = g(p, l)$ be the least integer which belongs* mod$p$ *to the exponent l. Then it is*

$$g(p, l) = O(l^{\varepsilon-1} \cdot p^{3/2}), \tag{15a}$$

for every positive ε.[10]

Proof. According to Theorem 2 the polynomial $x^{p-1} - a$ has (mod$p$) irreducible factors of degree l if and only if a belongs (mod$p$) to the exponent l. If g is the least integer with this property we have

$$\sigma_l(1) = \sigma_l(2) = \ldots = \sigma_l(g - 1) = 0.$$

According to Theorem 6 it holds

$$\sum_{a=1}^{g-1} \sigma_l(a) = \frac{1}{l} \sum_{t/l} \mu\left(\frac{l}{t}\right) \sum_{a=1}^{g-1} \sum_{j=0}^{d_t-1} \chi_j^{(t)}(a) = 0.$$

Since $d_t = (p - 1, p^t - 1) = p - 1$ for every t, we have

$$\sum_{t/l} \mu\left(\frac{l}{t}\right) \sum_{j=0}^{p-2} \sum_{a=1}^{g-1} \chi_j^{(t)}(a) = 0. \tag{16}$$

[10] The result is naturally not trivial only if l is of order greater then $p^{1/2+\varepsilon}$. Concerning the symbol O see footnote [4].

Let us establish the number of principal characters on the left-hand side of the equation (16). We have to find the number of integers divisible by $p - 1$ in the sequence

$$0, \frac{p^t - 1}{p - 1}, 2\frac{p^t - 1}{p - 1}, \ldots, (p - 2)\frac{p^t - 1}{p - 1}.$$

Since $\varkappa \frac{p^t - 1}{p - 1} \equiv \varkappa t \pmod{p - 1}$ it is sufficient to find how many of the integers

$$0, t, 2t, \ldots, (p - 2)\, t$$

are divisible by $p - 1$. Since further t/l, i. e. $t/p - 1$, this number is equal to the number of integers $\leqq p - 2$ (including 0) divisible by $\frac{p - 1}{t}$. Therefore, it is equal to t.

Hence, there exist among the $p - 1$ characters induced by

$$\chi_0^{(t)}, \chi_1^{(t)}, \ldots, \chi_{p-2}^{(t)}$$

in the group $\mathfrak{G}^{(1)}$ exactly t principal characters of the group $\mathfrak{G}^{(1)}$.

Let the divisors of the number l be $1 < t_2 < t_3 < \ldots < l$. The formula (16) has the explicit form

$$\sum_{a=1}^{g-1} \left\{ \mu\left(\frac{l}{1}\right) \sum_{j=1}^{p-1} \chi_j^{(1)}(a) + \mu\left(\frac{l}{t_2}\right) \sum_{j=1}^{p-1} \chi_j^{(t_2)}(a) + \ldots + \mu\left(\frac{l}{l}\right) \sum_{j=1}^{p-1} \chi_j^{(l)}(a) \right\} = 0.$$

The first sum in the bracket contains just one principal character, the second sum just t_2 principal characters, ..., the last sum just l principal characters.

We separate the principal characters

$$\sum_{a=1}^{g-1} \left\{ \mu\left(\frac{l}{1}\right) + t_2 \mu\left(\frac{l}{t_2}\right) + \ldots + l\mu\left(\frac{l}{l}\right) \right\} = - \sum_{a=1}^{g-1} \left\{ \mu\left(\frac{l}{1}\right) \sum{}' \chi_j^{(1)}(a) + \right.$$
$$\left. + \mu\left(\frac{l}{t_2}\right) \sum{}' \chi_j^{(t_2)}(a) + \ldots + \mu\left(\frac{l}{l}\right) \sum{}' \chi_j^{(l)}(a) \right\}.$$

The bracket on the left hand side is the EULER function $\varphi(l)$. The sign Σ' on the right hand side denotes that the sum extends to the non-principal characters.

Now we use the well-known estimation:[11])

If $p > 2$, $1 \leqq g < p$ there holds for every non-principal character (mod$p$)

$$\left| \sum_{n=1}^{g} \chi(n) \right| < \sqrt{p} \log p.$$

It is therefore

[11]) See e. g. LANDAU, Vorlesungen über Zahlentheorie II, 1927, p. 178.

$$\begin{aligned}\varphi(l)\,.\,(g-1) < {} & (p-1-1)\sqrt{p}\log p + \\ & + (p-1-t_2)\sqrt{p}\log p + \\ & \dots\dots\dots\dots\dots\dots \\ & + (p-1-l)\sqrt{p}\log p,\end{aligned}$$

i. e.

$$g-1 < \frac{1}{\varphi(l)}\,[T(l)\,.\,(p-1)-S(l)]\sqrt{p}\log p, \tag{18}$$

where $T(l)$ and $S(l)$ denote the number of divisors and the sum of divisors of l.

From (18) it follows further

$$g < \frac{T(l)}{\varphi(l)}\cdot p^{3/2}\log p.$$

Using the formulae:[12])

$$T(l) = O(l^{\frac{1}{2}\varepsilon}) \text{ for every positive } \varepsilon,$$

$$\varphi(l) > \frac{A\ .\,l}{\log\log l} \text{ with a positive constant } A, \tag{19}$$

we have

$$g(p, l) = O(l^{\frac{\varepsilon}{2}-1} p^{3/2}\log p). \tag{19a}$$

If $l < p^{1/2}$ the result (15a) is true but trivial, since $l^{\varepsilon-1}p^{3/2} > l^{\varepsilon}p$.

If $l > p^{1/2}$, $p^{\varepsilon/4} < l^{\varepsilon/2}$, $\log p = O(p^{\varepsilon/4})$, $\log p < c(\varepsilon)\,.\,l^{\varepsilon/2}$ with a constant $c(\varepsilon)$ depending only on ε. Therefore from (19a) follows

$$g(p, l) = O(l^{\varepsilon-1}\,.\,p^{3/2}).$$

This proves Theorem 7.

V.

We shall finally make a slight generalization of the former theory by considering binomial equations over an arbitrary finite field $G\,F(p^f)$ of degree f as ground field.

Let us denote $P = p^f$, $[P] = G\,F(p^f)$ and let us consider polynomials of the form

$$x^n - a,\ (n, p) = 1,\ a \in [P],\ a \neq 0. \tag{20}$$

We define[13])

$$D_t = (n, P^t - 1), \tag{21}$$

and

[12]) See, for instance: HARDY-WRIGHT, An Introduction to the Theory of numbers, 1945, p. 265.

[13]) In our previous notation it is clearly $D_t = d_{ft}$, $\Delta_t = \delta_{ft}$.

$$\varDelta_t = \begin{cases} 0 & \text{if } a^{\frac{P^t-1}{D_t}} \neq 1, \\ D_t & \text{if } a^{\frac{P^t-1}{D_t}} = 1, \end{cases} \tag{22}$$

where 1 denotes the unity element of the field $[P]$.

We can now state without detailed proof:

Generalization of Theorem 1. *Let* (20) *be a polynomial of degree n over the field $[P]$. Let t be an integer, $1 \leq t \leq n$, $\mu(t)$ the* Möbius *function, D_t and $\varDelta_t$ defined by* (21) *and* (22) *respectively. Let σ_k denote the number of irreducible factors of* (20) *of degree k in the field $[P]$. Then it holds*

$$\sigma_k = \frac{1}{k}\sum_{t/k}\mu\left(\frac{k}{t}\right)\varDelta_t,$$

where t runs through all divisors of k.

As a consequence of Theorem 1 the following theorem can be proved:

Generalization of Theorem 2. *Let $a \epsilon [P]$ belong to the exponent l. Then the polynomial $x^{P-1} - a$ is in $[P]$ a product of $\frac{P-1}{l}$ irreducible polynomials of degree l.*

As in section III we introduce the characters of the multiplicative group of the field $[P]$ and of its extension-fields $[P^t]$.

In our previous notation the multiplicative group of $[P^t]$ is $\mathfrak{G}^{(ft)}$, its principal character $\chi_0^{(ft)}$. There exist $P^t - 1$ different characters of the group $\mathfrak{G}^{(ft)}$. Moreover, there exist precisely D_t characters $\chi_j^{(ft)}$ for which

$$(\chi_j^{(ft)})^n = \chi_0^{(ft)}$$

holds. The element G being a generating element of the group $\mathfrak{G}^{(ft)}$ these D_t characters are given by the property

$$\chi_j^{(ft)}(G) = e^{\frac{2\pi i}{D_t}\cdot j} \quad (j = 0, 1, 2, \ldots, D_t - 1). \tag{23}$$

We find:

Generalization of Theorem 6. *Let the D_t characters $\chi_j^{(ft)}$ be defined by the relation* (23). *Then the number of irreducible factors of degree k of the polynomial* (20) *in $[P]$ is given by the formula*

$$\sigma_k(a) = \frac{1}{k}\sum_{t/k}\mu\left(\frac{k}{t}\right)\sum_{j=0}^{D_t-1}\chi_j^{(ft)}(a). \tag{24}$$

Using the formula (24) we shall prove a generalization of a result due to H. Davenport.[14]

[14] See l. c. [5] (cited according to the Zentralblatt **18** (1938), p. 109).

Davenport proved: To every integer f there exist an integer $p_0 = p_0(f)$ with the following property. Let be $p > p_0$, ϑ an arbitrary generating element of $G\,F(p^f)$ with respect to $G\,F(p)$. Then there exist an element $c \in G\,F(p)$ so that $\vartheta - c$ is a generating element of the multiplicative group of the field $[P]$ (i. e. a primitive root of the field $[P]$).

The proof of this result is based upon the following estimation of a character sum: For every generating element ϑ and every non-principal character χ of the field $[P]$ the following relation holds

$$\sum_{c=0}^{p-1} \chi(\vartheta + c) = O(p^{1-\frac{1}{2(f+1)}}). \tag{25}$$

We use Davenport's formula (25) to the proof of the following more general

Theorem 9. *Let be $f > 1$, $G\,F(p^f)$ a Galois field, ϑ an arbitrary generating element of $G\,F(p^f)$ with respect to $G\,F(p)$. Let further be: l an integer, $l/P - 1$, $P = p^f$, $l > K \,.\, P^{1-\frac{1}{2f(f+1)}+\varepsilon}$, $K > 0$, $\varepsilon > 0$ being two arbitrary constants. Then there exists a constant $p_0 = p_0(f, \varepsilon, K)$ with the following property: If $p > p_0$ it is always possible to find an element $c \in G\,F(p)$ so that $\vartheta - c$ belongs to the exponent l.*[15])

Proof. The polynomial $x^{P-1} - a$ has in $[P]$ irreducible factors of degree l if and only if a belongs to the exponent l.

We prove our Theorem indirectly. Let us suppose that none of the elements

$$\vartheta, \vartheta + 1, \vartheta + 2, \ldots, \vartheta + p - 1 \tag{26}$$

belongs to the exponent l. With respect to (24) we have

$$\sum_{c=0}^{p-1} \sigma_l(\vartheta + c) = 0,$$

i. e.

$$\sum_{c=0}^{p-1} \sum_{t/l} \mu\left(\frac{l}{t}\right) \sum_{j=0}^{D_t-1} \chi_j^{(ft)}(\vartheta + c) = 0,$$

and since $D_t = (P - 1, P^t - 1) = P - 1$,

$$\sum_{c=0}^{p-1} \sum_{t/l} \mu\left(\frac{l}{t}\right) \sum_{j=0}^{P-2} \chi_j^{(ft)}(\vartheta + c) = 0. \tag{27}$$

We shall prove that there exists a constant $p_0 = p_0(f, \varepsilon, K)$ so that for $p > p_0$, $l > K \,.\, P^{1-\frac{1}{2f(f+1)}+\varepsilon}$ the equation (27) cannot hold.

First it can be proved by a reasoning analogous to that used in the proof of Theorem 7: among the $P - 1$ characters

$$\chi_0^{(ft)}, \chi_1^{(ft)}, \ldots, \chi_{P-2}^{(ft)}$$

[15]) For $K = \frac{1}{2}$, $\varepsilon = \dfrac{1}{2f(f+1)}$ we have Davenport's result.

of the group $\mathfrak{G}^{(ft)}$ there exist exactly t characters which induce in the subgroup $\mathfrak{G}^{(f)}$ (multiplicative group of $[P]$) principal characters of $\mathfrak{G}^{(f)}$.

Let the divisors of l be: $1 < t_2 < t_3 < \ldots < l$. Separating the principal characters we write (27) in the form

$$\sum_{c=0}^{p-1}\left\{\mu\left(\frac{l}{1}\right) + t_2\mu\left(\frac{l}{t_2}\right) + \ldots + l\mu\left(\frac{l}{l}\right)\right\} = \varphi(l)\,.\,p =$$

$$= -\sum_{c=0}^{p-1}\left\{\mu\left(\frac{l}{1}\right)\sum_{j=1}^{P-2}{}' \chi_j^{(f)}(\vartheta + c) + \mu\left(\frac{l}{t_2}\right)\sum_{j=1}^{P-2}{}' \chi_j^{(ft_2)}(\vartheta + c) + \ldots + \right.$$

$$\left. + \mu\left(\frac{l}{l}\right)\sum_{j=1}^{P-2}{}' \chi_j^{(fl)}(\vartheta + c)\right\}.$$

The sign Σ' on the right hand side denotes that the sum extends to the non-principal characters. The first sum in the bracket contains $P - 2$ non-principal characters, the second sum $P - 1 - t_2$ non-principal characters, ..., the last sum $P - 1 - l$ non-principal characters.

With respect to (25) we have

$$p\,.\,\varphi(l) = O\left(T(l)\,.\,(P-1)\,.\,p^{1-\frac{1}{2(f+1)}}\right),$$

where $T(l)$ is the number of divisors of l. The constant implied by the symbol O depens only on f.

With respect to (19) we have further

$$p = O\left(T(l)\,.\,l^{-1}\,.\,\log\log l\,.\,P\,.\,p^{1-\frac{1}{2(f+1)}}\right).$$

Now one can write

$$T(l) = O(l^{\varepsilon/4}),\ \log\log l = O(l^{\varepsilon/4}),$$

the constants implied by O depending only on $\varepsilon > 0$. Therefore

$$p = O(l^{\varepsilon/2}\,.\,l^{-1}\,.\,p\,.\,P^{1-\frac{1}{2f(f+1)}}).$$

Finally it is $l^{\varepsilon/2} < P^{\varepsilon/2}$. Following to the supposition

$$l^{-1} < \frac{1}{K}\,.\,P^{-1+\frac{1}{2f(f+1)}-\varepsilon}$$

we would have therefore

$$p = O(P^{\varepsilon/2}\,.\,P^{-1+\frac{1}{2f(f+1)}-\varepsilon}\,.\,p\,.\,P^{1-\frac{1}{2f(f+1)}}),$$

$$p = O(p^{1-\frac{1}{2}\varepsilon f}). \tag{28}$$

The relation (28) shows that our assumption concerning the sequence (26) cannot hold for $p > p_0$, $p_0 = p_0(f, \varepsilon, K)$ sufficiently large. This proves our Theorem.

*

O rozložitelnosti binomických kongruencií a o najmenšom celom čísle patriacom k danému exponentu (mod$p$).

(Obsah predošlého článku.)

Nech je daná kongruencia (1). Nech σ_k značí počet ireducibilných faktorov k-tého stupňa kongruencie (1). Obsahom odstavcov I—III predloženej práce je určenie vzorcov pre číslo σ_k.

V odstavci I dokazujeme: Pre číslo $\sigma_k = \sigma_k(a)$ platí vzorec (1a), kde $\mu(t)$ je MÖBIUSOVA funkcia a čísla δ_t sú veličiny definované v textu.

V odstavci II podávame niekol'ko aplikácií vzorca (1a) na špeciálne kongruencie.

Obsahom odstavca III je dôkaz vzorca (13), v ktorom čísla $\chi_j^{(t)}$ značia isté, jednoznačne definované, charaktery multiplikatívnej grupy konečného telesa o p^t elementoch.

V odstavci IV dokazujeme pomocou vzorca (13) túto vetu: Nech l je celé číslo, $l/p - 1$. Nech $g = g(p, l)$ je najmenšie celé číslo patriace mod$p$ k indexu l. Potom je $g(p, l) = O(l^{\varepsilon - 1} . p^{3/2})$ pre každé $\varepsilon > 0$.

V odstavci V zovšeobecňujeme výsledky odstavcov I—III na binomické rovnice vo všeobecných konečných telesiach. Ako analogiu výsledku odstavca IV dokazujeme napokon túto vetu:

Nech $f > 1$, $G\,F(p^f)$ GALOISOVO pole, ϑ jeho l'ubovolný vytvorujúci element vzhl'adom k telesu $G\,F(p)$. Nech je ďalej: l celé číslo, $l/P - 1$, $P = p^f$, $K > 0$, $\varepsilon > 0$ dve l'ubovolné konštanty, $l > K . P^{1 - \frac{1}{2f(f+1)} + \varepsilon}$. Potom existuje taká konštanta $p_0 = p_0(f, \varepsilon, K)$, že pre $p > p_0$ možno nájsť vždy element $c \in G\,F(p)$ tej vlastnosti, že $\vartheta - c$ patrí k exponentu l.