

**Addendum and corrigendum to the paper  
"Abelian binomials, power residues and exponential  
congruences", Acta Arith. 32(1977), pp. 245-274**

by

A. SCHINZEL (Warszawa)

1. Dr J. Wójcik has pointed out that the equality in formula (28) which is only said to hold but not proved is actually used on p. 261 line 6. The equality in question follows from the formula displayed in the last line on p. 259, where also  $\leq$  can be replaced by  $=$ . The latter is a consequence of the fact that for  $q > 2$  the extension  $K(\zeta_{q^p})/K$  is cyclic and for  $q = 2, p \neq 2$  we have  $\text{ord}_p[K(\zeta_{q^p}) : K] = 0$ .

2. The remark made on p. 261 has not been proved rigorously, since it is not clear why  $\tau(\chi) \neq 0$ . Therefore, we return to the question and we shall prove more than was asserted namely that the number  $\sigma$  occurring in Theorem 3 is the least integer with the required property, provided  $(\sigma, n/w_n) = 1$ .

By the definition of  $\sigma$  there exists a character  $\chi$  belonging to the exponent  $\sigma$  on the group  $G = \text{Gal}(K(\zeta_n)/K)$  represented as a multiplicative group of residue classes mod  $n$ . Let

$$\tau_y = \sum_{x \in G} \chi(x) \zeta_n^{xy}.$$

Since  $\chi(x)$  are non-zero and the Vandermonde determinant  $|\zeta_n^{xy}|_{\substack{x \in G \\ y=1,2,\dots,|G|}}$  is non-zero there exists a  $y$  such that  $\tau_y \neq 0$ . Let us fix such a  $y$  and denote the corresponding  $\tau_y$  by  $\tau(\chi) \neq 0$ . Since  $\chi(x) \in K, \chi(x)^\sigma = 1$  we have  $\tau(\chi) \in K(\zeta_n), \tau(\chi)^\sigma \in K, \tau(\chi)^{n\sigma} \in K^n$ . Suppose that  $\tau(\chi)^{n\sigma} = \gamma^n, \gamma \in K$ . Then

$$\tau(\chi)^{\frac{n}{w_n} \sigma} = \zeta_{w_n}^a \gamma \in K$$

and applying an automorphism  $\zeta_n \rightarrow \zeta_n^j$  with  $j \in G$  we get

$$\tau(\chi)^{\frac{n}{w_n} \sigma} \bar{\chi}(j)^{\frac{n}{w_n} \sigma} = \tau(\chi)^{\frac{n}{w_n} \sigma}.$$

Since  $\tau(\chi) \neq 0$  it follows that

$$\chi(j)^{\frac{n}{w_n}} = 1$$

and by the choice of  $\chi$

$$\sigma \left| \frac{n}{w_n} \rho.$$

Hence if  $(\sigma, n/w_n) = 1$  we get  $\sigma | \rho$ . If  $(\sigma, n/w_n) \neq 1$   $\sigma$  need not be the least integer with the property asserted in Theorem 3. In particular if  $\zeta_4 \notin K$ ,  $n \equiv 0 \pmod{2^{\tau+1}}$ ,  $\sqrt{-(\zeta_{2^{\tau}} + \zeta_{2^{\tau}}^{-1} + 2)} \in K$ ,  $\sigma$  can be replaced by  $(w_n, \text{l.c.m. } [K(\zeta_q) : K])$ .

The remark on p. 263 remains valid on replacing  $(w_n, n/w_n)$  by  $(\sigma, n/w_n)$  which makes it stronger.

3. Theorem 6 has the following equivalent form much more useful in applications.

**THEOREM 7.** Let  $f_r(z_1, \dots, z_p)$  ( $1 \leq r \leq s$ ) be polynomials with coefficients in an algebraic number field  $K$  and  $a_{ij}$  ( $1 \leq i \leq p, 1 \leq j \leq q$ ) non-zero elements of  $K$ ,  $M$  a positive integer. If the system of equations

$$(1) \quad f_r(z_1, \dots, z_p) = 0 \quad (1 \leq r \leq s)$$

has only finitely many solutions in the complex field and the system of congruences

$$(2) \quad f_r \left( \prod_{j=1}^q a_{1j}^{x_j}, \dots, \prod_{j=1}^q a_{pj}^{x_j} \right) \equiv 0 \pmod{m} \quad (1 \leq r \leq s)$$

is soluble for all moduli  $m$  prime to  $M$  then the system of equations

$$(3) \quad f_r \left( \prod_{j=1}^q a_{1j}^{x_j}, \dots, \prod_{j=1}^q a_{pj}^{x_j} \right) = 0 \quad (1 \leq r \leq s)$$

is soluble in rational integers  $w_j$ .

**Proof.** Since the system (1) has only finitely many solutions they all lie in a finite extension  $K_1$  of  $K$ . Let them be  $(\beta_{h1}, \dots, \beta_{hp})$  ( $1 \leq h \leq g$ ). Thus we have the equivalence

$$\bigwedge_{r \leq s} f_r(z_1, \dots, z_p) = 0 \equiv \bigvee_{h \leq g} \bigwedge_{i \leq p} z_i = \beta_{hi}$$

and by the distributive property of alternative with respect to conjunction

$$(4) \quad \bigwedge_{r \leq s} f_r(z_1, \dots, z_p) = 0 \equiv \bigwedge_{i_1 \leq p} \bigwedge_{i_2 \leq p} \dots \bigwedge_{i_g \leq p} \bigvee_{h \leq g} z_{i_h} = \beta_{hi_h} \\ \equiv \bigwedge_{i_1 \leq p} \bigwedge_{i_2 \leq p} \dots \bigwedge_{i_g \leq p} \prod_{h=1}^g (z_{i_h} - \beta_{hi_h}) = 0.$$

By the Hilbert theorem on zeros it follows that for every integral vector  $i = [i_1, \dots, i_g] \in \{1, 2, \dots, p\}^g = I$  and a suitable exponent  $e_i$  we have

$$(5) \quad \prod_{h=1}^g (z_{i_h} - \beta_{hi_h})^{e_i} = \sum_{r=1}^s f_r(z_1, \dots, z_p) F_{ri}(z_1, \dots, z_p),$$

where  $F_{ri} \in K_1[z_1, \dots, z_p]$ . If  $m$  is prime to the denominators of  $F_{ri}$  and to the numerators as well as the denominators of  $a_{ij}$  the system of congruences (2) with  $m = m^e$ ,  $e = \max_{i \in I} e_i$ , and the identity (5) imply

$$(6) \quad \prod_{h=1}^g \left( \prod_{j=1}^q a_{i_h j}^{x_j} - \beta_{hi_h} \right) \equiv 0 \pmod{m} \quad (i \in I).$$

Therefore, the system (6) is soluble for all moduli prime to  $D = M$  times a certain finite product. Applying Theorem 6 we infer that the system of equations

$$\prod_{h=1}^g \left( \prod_{j=1}^q a_{i_h j}^{x_j} - \beta_{hi_h} \right) = 0 \quad (i \in I)$$

is soluble in integers. By the equivalence (4) this system is equivalent to (3) and the proof is complete.

A list of misprints is given below

p. 248 in many places for  $K$  read  $K^*$

line -18 for  $K(\xi)^p$  read  $K(\xi^p)$

line -15 for  $K(\xi)^2$  read  $K(\xi^2)$

line -9 for  $K^*$  read  $K$

line -7 after  $p = 2$  insert  $\zeta_4 \notin K$

line -4 for 2 read twice  $p$

line -3 for  $\eta^2 \in K\langle \xi \rangle$  or read  $\eta^p \in K^*\langle \xi \rangle$  or  $p = 2$ ,  $\zeta_4 \notin K$  and

p. 249 line 13 for  $\tau+1$  read  $\tau$ , in the second paranthesis insert  $+2$ ,

p. 250 line -1 for  $= \alpha^{2^{\mu}}$  read  $\alpha^{2^{\mu}-1}$

line 10 for  $p^{\mu-n}$  read  $p^{\mu-n}j$

line 11 for  $\delta^{-1}$  read  $\delta^{-j}$

p. 251 formula (13) for  $\tau-1$  read  $2^{\tau-1}$

formula (14) for  $\nu-2$  read  $2^{\nu-2}$

p. 253 line 11 for  $\omega$  read  $\omega > 0$

p. 255 line -13 for  $\nu$  read  $\tau$

p. 255 formula (18) for  $\tau$  read  $\nu$

p. 256 lines -5, -3 for  $\gamma$  read  $\gamma_1$

p. 257 line 12 for  $\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1} + 2$  read  $\zeta_{2^{\tau}} + \zeta_{2^{\tau}}^{-1} + 2$

p. 259 formula (27) for  $\gamma \zeta_p^j$  read  $\gamma \zeta_p^j$

p. 259 line -15 for [2] read [2] for char  $K = 0$

p. 261 line 3 for  $p > 2$  read  $p > 2$

p. 263 line 14 for  $e_0$  read  $e_0$

p. 264 formula (43) for  $j = 1$  read  $s = 1$

p. 265 line -2 for  $\alpha_i$  read  $\alpha_k$ , for  $n'$  read  $n$

- p. 266 line -7 for  $(w, c_{r+1}, \dots, c_k)$  read  $(w, c_{r+1}, \dots, c_k)_{t_s}$   
 line -3 for  $t_1$  read  $t_0$   
 line -2 before mod insert  $\equiv 0$
- p. 267 formula (46) for  $j = 1$  read  $s = 1$ , for  $\equiv 0$  read  $\equiv 0 \pmod n$
- p. 268 line 15 for  $f(a_1^{x_1}, a_2^{x_2})$  read  $f(a_1^{x_1} a_2^{x_2})$   
 line -7 for  $u_n = \lambda_1 \alpha^n + \lambda_2 \alpha^{-n}$  read  $u_n = \lambda_1 \alpha^n + \lambda_2 \alpha^{-n}$
- p. 272 line 9 for  $Znám$  read  $Znám$  [11]
- p. 273 line -2 for  $b_{n_i}$  read  $b_{n_i}$

Les volumes IV et suivants sont à obtenir chez	Volumes from IV on are available at	Die Bände IV und folgende sind zu beziehen durch	Томы IV и сле- дующие можно получить через
--	---	--	--

Ars Polona, Krakowskie Przedmieście 7, 00-068 Warszawa

Les volumes I-III sont à obtenir chez	Volumes I-III are available at	Die Bände I-III sind zu beziehen durch	Томы I-III можно получить через
--	-----------------------------------	---	------------------------------------

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

BOOKS PUBLISHED BY THE POLISH ACADEMY OF SCIENCES  
INSTITUTE OF MATHEMATICS

- S. Banach, Oeuvres, vol. II, 1979, 470 pp.  
 S. Mazurkiewicz, Travaux de topologie et ses applications, 1969, 380 pp.  
 W. Sierpiński, Oeuvres choisies, vol. I, 1974, 300 pp.; vol. II, 1975, 780 pp.; vol. III, 1976, 688 pp.  
 J. P. Schauder, Oeuvres, 1978, 487 pp.  
 H. Steinhaus, Selected papers, in print.  
 Proceedings of the Symposium to honour Jerzy Neyman, 1977, 349 pp.

MONOGRAFIE MATEMATYCZNE

27. K. Kuratowski, A. Mostowski, Teoria mnogości, 5 th ed. 1978, 470 pp.  
 43. J. Szarski, Differential inequalities, 2nd ed., 1967, 256 pp.  
 44. K. Borsuk, Theory of retracts, 1967, 251 pp.  
 47. D. Przeworska-Rolewicz and S. Rolewicz, Equations in linear spaces, 1968, 380 pp.  
 50. K. Borsuk, Multidimensional analytic geometry, 1969, 443 pp.  
 51. R. Sikorski, Advanced calculus. Functions of several variables, 1969, 460 pp.  
 57. W. Narkiewicz, Elementary and analytic theory of algebraic numbers, 1974, 630 pp.  
 58. C. Bessaga and A. Pełczyński, Selected topics in infinite-dimensional topology, 1975, 353 pp.  
 59. K. Borsuk, Theory of shape, 1975, 379 pp.  
 60. R. Engelking, General topology, 1977, 626 pp.  
 61. J. Dugundji and A. Granas, Fixed point theory, vol. I, in print.

BANACH CENTER PUBLICATIONS

- Vol. 1. Mathematical control theory, 1976, 166 pp.  
 Vol. 2. Mathematical foundations of computer science, 1977, 259 pp.  
 Vol. 3. Mathematical models and numerical methods, 1978, 391 pp.  
 Vol. 4. Approximation theory, 1979, 314 pp.  
 Vol. 5. Probability theory, 1979, 289 pp.  
 Vol. 6. Mathematical statistics, in print.  
 Vol. 7. Discrete mathematics, in print.  
 Vol. 8. Spectral theory, in print.  
 Vol. 9. Universal algebra and applications, in print.