ACTA ARITHMETICA
XXXVI (1980)

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 $\leqslant$ can be replaced by $=$. The latter is a consequence of the fact that for $q > 2$ the extension $K(\zeta_{q^s})/K$ is cyclic and for $q = 2$, $p \neq 2$ we have $\operatorname{ord}_p[K(\zeta_{q^s}) : K] = 0$.

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 σ occurring in Theorem 3 is the least integer with the required property, provided $(\sigma, n/w_n) = 1$.

By the definition of σ there exists a character χ belonging to the exponent σ on the group $G = \operatorname{Gal}(K(\zeta_n)/K)$ 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 $|\zeta_n^{xy}|_{\substack{x \in G \\ y=1,2,\ldots,|G|}}$ is non-zero there exists a y such that $\tau_y \neq 0$. Let us fix such a y and denote the corresponding τ_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 $\tau(\chi)^{nq} = \gamma^n$, $\gamma \in K$. Then

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

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

$$\tau(\chi)^{\frac{n}{w_n}q}\,\overline{\chi}(j)^{\frac{n}{w_n}q} = \tau(\chi)^{\frac{n}{w_n}q}.$$

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

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

and by the choice of χ

$$\sigma \Big| \frac{n}{w_n} \varrho.$$

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

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

$$f_r(z_1, \ldots, z_p) = 0 \quad (1 \leqslant r \leqslant s) \tag{1}$$

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

$$f_r\Big(\prod_{j=1}^{q} a_{1j}^{x_j}, \ldots, \prod_{j=1}^{q} a_{pj}^{x_j}\Big) \equiv 0 \bmod m \quad (1 \leqslant r \leqslant s) \tag{2}$$

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

$$f_r\Big(\prod_{j=1}^{q} a_{1j}^{x_j}, \ldots, \prod_{j=1}^{q} a_{pj}^{x_j}\Big) = 0 \quad (1 \leqslant r \leqslant s) \tag{3}$$

is soluble in rational integers x_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 $(\beta_{h1}, \ldots, \beta_{hp})$ $(1 \leqslant h \leqslant g)$. Thus we have the equivalence

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

and by the distributive property of alternative with respect to conjunction

$$\bigwedge_{r \leqslant s} f_r(z_1, \ldots, z_p) = 0 \equiv \bigwedge_{i_1 \leqslant p} \bigwedge_{i_2 \leqslant p} \ldots \bigwedge_{i_g \leqslant p} \bigvee_{h \leqslant g} z_{i_h} = \beta_{hi_h} \tag{4}$$

$$\equiv \bigwedge_{i_1 \leqslant p} \bigwedge_{i_2 \leqslant p} \ldots \bigwedge_{i_g \leqslant p} \prod_{h=1}^{g} (z_{i_h} - \beta_{hi_h}) = 0.$$

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

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

where $F_{ri} \in K_1[z_1, \ldots, z_p]$. If $\mathfrak{m}$ 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 $m = \mathfrak{m}^e$, $e = \max_{i \in I} e_i$, and the identity (5) imply

$$\prod_{\substack{h=1 \\ \beta_{hi_h} \neq 0}}^{g} \Big(\prod_{j=1}^{q} a_{i_h j}^{x_j} - \beta_{hi_h} \Big) \equiv 0 \bmod \mathfrak{m} \quad (\boldsymbol{i} \in I). \tag{6}$$

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

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

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 τ, in the second paranthesis insert $+2$,
p. 250 line −1 for $= \alpha^{2^\mu}$ read $\alpha^{2^{\mu-1}}$
line 10 for $p^{\mu-\kappa}$ read $p^{\mu-\kappa}j$
line 11 for δ^{-1} read δ^{-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 ω read $\omega > 0$
p. 255 line −13 for ν read r
p. 255 formula (18) for τ read ν
p. 256 lines −5, −3 for γ read γ_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 $\gamma\zeta_p{}^{\nu}$ read $\gamma\zeta_p{}^{j\nu}$
p. 259 line −15 for [2] read [2] for $\operatorname{char} K = 0$
p. 261 line 3 for $p \geqslant 2$ read $p > 2$
p. 263 line 14 for c_0 read e_0
p. 264 formula (43) for $j = 1$ read $s = 1$
p. 265 line −2 for c_l read c_k, for n' read n

p. 266 line −7 for $(w, c_{r+1}, \ldots, c_k)$ read $(w, c_{r+1}, \ldots, c_k)t_s$
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 $= 0$ read $\equiv 0 \bmod n$
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 $b_{h_i ir}$ read $b_{h_i is}$
