

## 6. WHAT ABOUT q?

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **43 (1997)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

### **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

6. WHAT ABOUT  $q$  ?

We pose the question: is  $q$  necessarily a  $q^s$ th power modulo  $p$  in Theorem 2? A numerical test will quickly show that this is most certainly not always so. However, Theorem 3 tells us that the answer is in fact “yes” in most cases.

*Proof of Theorem 3.* Let  $K, L, \pi$  be as in the proof of Theorem 2 and assume  $s > 0$ . Note first that  $(q/\pi)_l = (\pi, q)_l$  by reciprocity law (6). We will evaluate the latter symbol.

Viewing  $\Phi_{n/l}(X, Y)$  as a polynomial over  $K$ , we have that

$$\pi = N_{L/K}(y - qx\zeta_n) = \Phi_{n/l}(y, qx\zeta_l),$$

where  $\zeta_l$  in this equation is given by  $\zeta_l^{n/l} = \zeta_n^{n/l}$ . We now state the following generating formula for homogeneous cyclotomic polynomials:

$$(8) \quad \Phi_m(X, Y) = \frac{X^m - Y^m}{\prod_{\substack{d|m \\ 0 < d < m}} \Phi_d(X, Y)}.$$

Applying this formula recursively, we see that  $\pi$  is expressible as a product of numbers of the form  $y^r - (qx\zeta_l)^r$  and reciprocals of such numbers, where  $r$  is some positive divisor of  $n/l$ . To show that  $(\pi, q)_l = 1$ , it is by bimultiplicativity enough to show that  $(y^r - (qx\zeta_l)^r, q)_l = 1$  for all such  $r$ . And since  $n/l$  is relatively prime to  $q$ , it will clearly suffice to show that  $(y - qx\zeta_l, q)_l = 1$  for any choice of  $\zeta_l$  and integers  $x$  and  $y$  with  $y$  relatively prime to  $q$ .

We have

$$(y - qx\zeta_l, q)_l = (y, q)_l (1 - qxy^{-1}\zeta_l, q)_l.$$

The first symbol  $(y, q)_l$  is fixed under the action of the Galois group  $G_{\mathbf{Q}_q(\zeta_l)/\mathbf{Q}_q}$  by Theorem 6(h) since  $y, q \in \mathbf{Q}_q$ . As an  $l$ th root of unity with  $l$  odd, it must therefore be 1.

By Theorem 6(f),  $(1 - qxy^{-1}\zeta_l, qxy^{-1}\zeta_l)_l = 1$ . But by bimultiplicativity, this means that

$$(1 - qxy^{-1}\zeta_l, q)_l = (1 - qxy^{-1}\zeta_l, xy^{-1})_l^{-1} (1 - qxy^{-1}\zeta_l, \zeta_l)_l^{-1}.$$

Corollary 8 yields that  $1 - qxy^{-1}\zeta_l \equiv 1 \pmod{f_l(xy^{-1})}$ , and so the first symbol on the right is 1. The second symbol can be evaluated by turning it back into a power residue symbol and applying (4). Since  $\zeta_l$  is a unit in the ring of integers of  $K$ , the reciprocity law (5) yields

$$(9) \quad (1 - qxy^{-1}\zeta_l, \zeta_l)_l = \left( \frac{\zeta_l}{1 - qxy^{-1}\zeta_l} \right)_l = \zeta_l^{(N_K(1 - qxy^{-1}\zeta_l) - 1)/l}.$$

Thus  $(1 - qxy^{-1}\zeta_l, \zeta_l)_l$  will equal 1 if and only if  $N_K(1 - qxy^{-1}\zeta_l) \equiv 1 \pmod{q^{2s}}$ . In fact,

$$N_K(1 - qxy^{-1}\zeta_l) = \sum_{i=0}^{q-1} (qxy^{-1})^{iq^{s-1}} \equiv 1 \pmod{q^{q^{s-1}}}.$$

It is easily seen that  $q^{s-1} \geq 2s$  exactly when stated in the theorem. □

One remark on the case  $s = 1$ . If in fact we take  $n = q$ , then since  $\Phi_q(X) = 1 + X + \dots + X^{q-1}$  we have that  $p \equiv 1 \pmod{q^2}$  if and only if  $q$  divides  $x$ . Then  $q$  is a  $q$ th power modulo  $p$  if and only if  $x$  is divisible by  $q$ , in stark contrast to the above theorem.

### 7. THE EVEN CASE

We now turn to the case of  $q = 2$ . Given a positive integer  $s$ , let us set  $l = 2^s$ . We refrain from proving the theorem for the more general case of homogeneous polynomials, though it holds under such a generalization.

Any  $\alpha \in \mathbf{Q}_2^*$  may be written uniquely as  $\alpha = \xi 2^b(-3)^c$  where  $\xi = \pm 1$ ,  $b \in \mathbf{Z}$ , and  $c \in \mathbf{Z}_2$ . Note that  $b = v_2(\alpha)$ , where  $v_2$  is the 2-adic valuation. Denote by  $f_l(\alpha)$  the conductor of the norm residue character  $(\cdot, \alpha)_l$  in  $\mathbf{Q}_2(\zeta_l)$ . The conductors in this case have been worked out by Despina Prapavessi in [P]. We use a corrected version of her theorem [Sh1].

**THEOREM 9 (Prapavessi).** *Let  $\alpha \in \mathbf{Q}_2^*$  and write  $\alpha = \xi 2^b(-3)^c$  as above. Let  $w = \min \{v_2(b), v_2(c) + 2\}$ . Then if  $\xi = 1$ ,*

$$f_l(\alpha) = \begin{cases} (8) & \text{if } w = 0, \\ (4) & \text{if } w = 1 \text{ and } s \geq 2, \\ (\lambda_{2^{w-1}}) & \text{if } 2 \leq w \leq s \text{ and } w = v_2(c) + 2, \\ (\lambda_{2^w} \lambda_{2^{w+1}}) & \text{if } 2 \leq w < s - 1 \text{ and } w \leq v_2(c) + 1, \\ (\lambda_{2^{s-1}}) & \text{if } 2 \leq w = s - 1 \text{ and } w = v_2(c) + 1, \\ (1) & \text{otherwise.} \end{cases}$$