Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 43 (1997)

Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ON CYCLOTOMIC POLYNOMIALS, POWER RESIDUES, AND RECIPROCITY LAWS

Autor: Sharifi, Romyar T.

Kapitel: 6. WHAT ABOUT q?

DOI: https://doi.org/10.5169/seals-63283

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 14.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

6. What about q?

We pose the question: is q necessarily a q^sth 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, π 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 ζ_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:

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

Applying this formula recursively, we see that π 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 ζ_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 lth 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 $1 - qxy^{-1}\zeta_l \equiv 1 \mod \mathfrak{f}_l(xy^{-1})$, 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 ζ_l is a unit in the ring of integers of K, the reciprocity law (5) yields

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

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

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

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 $\Phi_q(X) = 1 + X + \cdots + X^{q-1}$ we have that $p \equiv 1 \bmod q^2$ if and only if q divides x. Then q is a qth 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 $\mathfrak{f}_l(\alpha)$ 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 $\xi = 1$,*

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