Revista de la
Unión Matemática Argentina
Volumen 28, 1976.

ON k-TH POWER RESIDUACITY

Pascual Llorente

INTRODUCTION. It is the purpose of this paper to generalize some results on k-th power residuacity presenting simpler and more conceptual proofs of those results.

In Section 2 a criterion for k-th power residuacity is given. This criterion generalizes the one obtained by E. Lehmer [3]. In Section 3 a simple solution to one problem considered by Sylvester [5] and E. Lehmer [4] and already essentially solved by Kummer [1] is given. They all focus their attention on the period equation and obtain their results using congruence properties of its roots. In this paper we consider the corresponding algebraic numbers field and obtain more general results using two simple lemmas presented in Section 1.

In the last section a criterion for the k-th character of 2 and 3 which generalizes the one obtained by E. Lehmer [2] for the case k=5 is given.

We thanks Dr. Marcos Sebastiani for the fruitful talks we kept during the preparation of this paper.

1. TWO LEMMAS, NOTATIONS AND SOME DEFINITIONS.

LEMMA 1. *Let* K *be an algebraic number field,* E/K *a cyclic extension of degree* n = k.r *and* F/K *the unique sub-extension of* E/K *of degree* k. *Let* q *be a prime ideal of* K *which factors in* E *as a product of* t *different prime ideals. Then* q *decomposes totally over* F *if and only if* k/t.

Proof. Let $q = Q_1 \ldots Q_t$ and $q = Q_1 \ldots Q_s$ be the decomposition of q as a product of prime ideals in E and F respectively, and suppose that $q \subset Q_1 \subset Q_1$. Clearly, since s/t and q decomposes totally over F (i.e. s=k), then k/t.

Conversely, let's suppose that k/t. Let $D_1 \subset G = Gal(E/K)$ be the decomposition group of Q_1 over K. Then $o(G/D_1) = t$ and $o(D_1)/r$. Then $D_1 \subset H = Gal(E/F)$ and D_1 is the decomposition group of Q_1 over F. Since $o(H/D_1) = r/o(D_1) = t/k$, then Q_1 factors as a product of t/k distinct prime factors in E. Since E/K is an abelian

extension, the decomposition groups of Q_i (i = 1,...,t) over K coincide with D_1. Then t = (t/k).s and s = k, i.e. q decomposes totally over F.

Now we fix the following notation:

Z	is the ring of integers
Q	is the rational number field
k, r, p and q	are positive integers such that $k > 2$
$p = k.r + 1$	is a prime number
$q \neq p$	and q is prime
Z_q (idem Z_p)	is the field Z/qZ (idem Z/pZ)
Q_q	is the field of q-adic numbers
g	is a generator (primitive root) for the multiplicative group of Z_p
θ_p	is a p-th primitive complex root of 1

$\eta_0(k,p), \eta_1(k,p),\ldots, \eta_{k-1}(k,p)$ are the so called r-nomial periods,

i.e. $\eta_i(k,p) = \sum_{t=0}^{r-1} \theta_p g^{kt+i}$ (i=0,...,k-1)

$E(p) = Q(\theta_p)$	is the cyclotomic field, which is a cyclic extension of Q of degree k.r
$F_k(p) = Q(\eta_0(k,p))$	is, then, the only sub-extension of degree k of the extension $E(p)/Q$.

Finally, for all $n \in Z$ such that $n \not\equiv 0 \pmod p$ we denote

$(n/p)_k = 1$	if the equation $z^k \equiv n \pmod p$ has a solution (i.e. if n is a k-th power residue mod p).

Most of our results are valid for k=2, but since the case of quadratic residues is very well known, for convenience, we suppose $k > 2$.

DEFINITION 1. We say that $h_k(p,x)$ is an equation associated to $F_k(p)$ if it is the minimal polynomial for some entire primitive number of the extension $F_k(p)/Q$.

In particular, the polynomial

$$f_k(p,x) = x^k + c_1(p)\, x^{k-1} + \ldots + c_k(p) \tag{1}$$

with roots $\eta_0(k,p),\ldots,\eta_{k-1}(k,p)$ (equation of the periods) is an equation associated to $F_k(p)$. It is known that

$$c_1(p) = 1 \tag{2}$$

and, if $(-1/p)_k = 1$ (which is always the case if k is odd), then

$$c_2(p) = -[(k-1)/2]\, r \tag{3}$$

Every equation $h_k(p,x)$ associated to $F_k(p)$ can be considered, in a natural fashion, as a polynomial in $\mathcal{Q}_q[x]$, and also as a polynomial in $Z_q[x]$. It is clear that if $h_k(p,x)$ has a root in $\mathcal{Q}_q$, then it has also a root in Z_q. The converse is not true in general.

DEFINITION 2. Let $h_k(p,x)$ be an equation associated to $F_k(p)$. We say that q is an exceptional prime if $h_k(p,x)$ has a root in Z_q but not in $\mathcal{Q}_q$.

LEMMA 2. *Let* $h_k(p,x)$ *be an equation associated to* $F_k(p)$.

(i) *If* $h_k(p,x)$ *has a single root in* Z_q *then* q *is not an exceptional prime for* $h_k(p,x)$. *Therefore, every exceptional prime for* $h_k(p,x)$ *divides the discriminant of* $h_k(p,x)$.

(ii) *Let* k *be a prime. If* q *is an exceptional prime for* $h_k(p,x)$ *then* $h_k(p,x)$ *has a single root in* Z_q, *i.e., there exists* $a \in Z$ *such that*

$$h_k(p,x) \equiv (x - a)^k \pmod{q}.$$

Proof. Lemma 2 follows immediately from Hensel Lemma. For (ii) observe that $h_k(p,x)$ factors in $\mathcal{Q}_q[x]$ then, necessarily it factors linearly.

2. CRITERION FOR k-TH POWER RESIDUACITY.

Kummer [1] proved that if $(q/p)_k = 1$ then $f_k(p,x)$ decomposes in k linear factors in $Z_q[x]$. The converse was proved by E. Lehmer [3] for all prime q such that q does not divide the discriminant of $f_k(p,x)$, using congruencial properties of the periods $\eta_i(k,p)$. She obtained the following criterion for k-th power residuacity:

"$(q/p)_k = 1$ *if and only if* $f_k(p,x)$ *has a root in* Z_q, *provided* q *does not divide the discriminant of* $f_k(p,x)$".

The following theorem shows that such criterion is not related to the equation of the periods but it is to the field $F_k(p)$, and that it holds for all prime q not exceptional.

THEOREM 1. (Criterion for k-th power residuacity).
Let $h_k(p,x)$ *be an equation associated to* $F_k(p)$. *Then* $(q/p)_k = 1$ *if and only if* $h_k(p,x)$ *has a root in* Z_q, *provided that* q *is not an exceptional prime for* $h_k(p,x)$.

Proof. Since $q \neq p$, q is unramified in E(p). Let $(q) = \mathcal{Q}_1 \ldots \mathcal{Q}_t$ be the factorization of the ideal (q) in prime ideals of E(p) and let f be the residual degree of the ideals $\mathcal{Q}_i$ (i=1,2,...,t). Then

$t.f = p - 1 = k.r.$

The theorem is proved considering the following chain of logic equivalences:

$(q/p)_k = 1 \longleftrightarrow q^r \equiv 1 \pmod p \longleftrightarrow f/r \longleftrightarrow k/t \longleftrightarrow$ (q) decomposes totally in $F_k(p) \longleftrightarrow h_k(p,x)$ factors linearly in $\mathbb{Q}_q[x] \longleftrightarrow h_k(p,x)$ has a root in $\mathbb{Q}_q \longleftrightarrow h_k(p,x)$ has a root in $\mathbb{Z}_q$.

where the fourth equivalence follows from Lemma 1, the last one follows from the fact that q is not an exceptional prime for $h_k(p,x)$, and the others follow immediately from well known results.

The above criterion is particularly interesting in case k is a prime. Then, by Lemma 2 ii) we have

COROLLARY 1. *Let* k *be a prime and* $h_k(p,x) = x^k + b_1(p)\, x^{k-1} + \ldots + b_k(p)$, *an equation associated to* $F_k(p)$. *If* $b_k(p) \equiv 0 \pmod q$ *and* $b_i(p) \not\equiv 0 \pmod q$ *for some* $i = 1,\ldots,k-1$, *then* $(q/p)_k = 1$.

In particular we have (recalling (2))

COROLLARY 1'. *Let* k *be a prime. If* $c_k(p) \equiv 0 \pmod q$, *then* $(q/p)_k = 1$.

However the equation of periods has a much more important property, which is a consequence of the following general result:

THEOREM 2. *Let* k *be a prime and* $h_k(p,x)$ *an equation associated to* $F_k(p)$ *such that its roots* $\alpha_1,\ldots,\alpha_k$ *form a basis for the integers of* $F_k(p)$. *Then:*

i) *For no prime* q *there exists an integer* $a \in \mathbb{Z}$ *such that*

$$h_k(p,x) \equiv (x - a)^k \pmod q$$

ii) $h_k(p,x)$ *has no exceptional primes.*

Proof. Let's suppose there is a prime q and an integer $a \in \mathbb{Z}$ such that

$$h_k(p,x) \equiv (x - a)^k \pmod q \tag{4}$$

Since k is a prime and $q \neq p$, it is clear that the ideal (q) is either prime in $F_k(p)$ or decomposes totally as a product of k distinct prime ideals of $F_k(p)$. In any case, clearly it follows from (4) that $q/(\alpha_i - a)$ $(i=1,\ldots,k)$ in the ring of integers of $F_k(p)$, which is impossible. Then our assumption (4) is false and Part i) of the theorem is proved.

Part ii) of the theorem follows immediately from Part i) and Lemma 2, ii).

Observing that the period equation $f_k(p,x)$ satisfies the hypothesis

of Theorem 2, one obtains:

COROLLARY 2. *Let* k *be a prime. Then:*

i) *For no prime* q *there exists an integer* $a \in Z$ *such that*

$$f_k(p,x) \equiv (x - a)^k \pmod{q}.$$

ii) $f_k(p,x)$ *has no exceptional primes.*

From this result and Theorem 1, one follows:

COROLLARY 3. *Let* k *be a prime. Then,* $(q/p)_k = 1$ *if and only if* $f_k(p,x)$ *has a root in* Z_q.

From these results it is possible to obtain more explicit criteria for k-th power residuacity for those k such that some equation $h_k(p,x)$ associated to $F_k(p)$ be known. To calculate such an equation seems to be a very difficult problem. The casesk = 3,4 has been completely studied in [3].

3. ON THE DIVISORS OF THE DISCRIMINANT OF AN EQUATION ASSOCIATED TO $F_k(p)$.

In this section we shall suppose k prime.

Observing E. Lehmer's criterion for k-th power residuacity in [3], one finds natural to ask on the k-th character (mod p) of the prime divisors of the discriminant $D_k(p)$ of the period equation $f_k(p,x)$. She considered this problem in [4], where she remarks that it was posed by Sylvester in [5], although essentially it had already been solved by Kummer in [1]. Following Kummer's ideas, that is to say, using congruential properties of the periods $\eta_i(k,p)$, she proves in [4]:

THEOREM 3. (Kummer - Lehmer). *If* $D_k(p) \equiv 0 \pmod{q}$ *then* $(q/p)_k = 1$.

Here we give a very simple proof of the following general result:

THEOREM 4. *Let* D *be the discriminant of an equation* $h_k(p,x)$ *associated to* $F_k(p)$. *If* q *is not an exceptional prime for* $h_k(p,x)$ *and if* $D \equiv 0 \pmod{q}$, *then* $(q/p)_k = 1$.

Proof. By hypothesis $h_k(p,x)$ has a non-trivial factorization in $Z_q[x]$. If any of these factors were linear, $h_k(p,x)$ would be the product of two coprime non-constant monic polynomials in $Z_q[x]$ and, by Hensel's Lemma, $h_k(p,x)$ would be reducible in $Q_q[x]$. Since $F_k(p)$ is an abelian extension of Q of prime degree k, $h_k(p,x)$ would

have a linear factorization in $Q_q[x]$ and, therefore, also in $Z_q[x]$, which is a contradiction. Then $h_k(p,x)$ has a root in Z_q and thus Theorem 4 follows from Theorem 1.

By Corollary 2, ii), it is clear that Theorem 3 is a particular case of Theorem 4.

It is interesting to consider the reciprocal of Theorems 3 and 4. In [4], using a known expression for $D_5(p)$ and some criteria for the quintic character of 2, 3, 5 and 7, it is proved the following:

THEOREM 5. (Lehmer). *If* $q = 2, 3, 5$ *or* 7, *then* $D_5(p) \equiv 0 \pmod q$ *if and only if* $(q/p)_5 = 1$.

Here we prove the following general result:

THEOREM 6. *Let* D *be the discriminant of an equation* $h_k(p,x)$ *associated to* $F_k(p)$. *If* $q < k$ *is not an exceptional prime for* $h_k(p,x)$, *then* $D \equiv 0 \pmod q$ *if and only if* $(q/p)_k = 1$.

Proof. If $D \equiv 0 \pmod q$ then $(q/p)_k = 1$ (Theorem 4). Reciprocally, if $(q/p)_k = 1$ then $h_k(p,x)$ has a linear factorization in $Z_q[x]$ and, since $q < k$, it is clear that $h_k(p,x)$ must have multiple roots in Z_q. Therefore $D \equiv 0 \pmod q$.

For the period equation we have:

THEOREM 7. *If* $q \leqslant k$, *then* $D_k(p) \equiv 0 \pmod q$ *if and only if* $(q/p)_k = 1$.

Proof. If $q < k$ the theorem follows from Theorem 6 and Corollary 2,ii). If $q = k$, one proves (as in the proof of Theorem 6 and remembering (2)) that $f_k(p,x)$ cannot have k different roots in Z_q, because in this case $1 = c_1(p) \equiv 0 \pmod q$. Then $D_k(p) \equiv 0 \pmod q$.

The case k=5 and q=7 of Theorem 5 (which is not included in Theorem 7) can be easily deduced from our preceding results using a known expression for the coefficients of $F_5(p,x)$ (see [2]). We don't give here the proof, not only because it is extraneous to the spirit of this paper, but also because we have evidence to suppose that Theorem 7 may be generalized in order to include Theorem 5. In a future communication we will consider the validity of Theorem 7 for primes $q > k$.

4. THE k-TH CHARACTER OF 2 AND 3.

E. Lehmer [2] gives some criteria for the quintic character of 2 and 3 (mod p) in terms of the representation of p by certain quadratic forms. Using these criteria and studying the constant term $c_5(p)$ of the period equation $f_5(p,x)$, she obtains the following result:

$$(2/p)_5 = 1 \text{ if and only if } c_5(p) \equiv 0 \pmod 2 \text{ and}$$
$$(3/p)_5 = 1 \text{ if and only if } c_5(p) \equiv 0 \pmod 3.$$

We generalize this result in the following way:

THEOREM 8. *For any prime* $k > 2$, 2 *is a* k-th *power residue of a prime* $p = k.r + 1$ *if and only if* $c_k(p) \equiv 0 \pmod 2$.

Proof. We have seen (Corollary 1') that if $c_k(p) \equiv 0 \pmod 2$, then $(2/p)_k = 1$. Reciprocally, if $(2/p)_k = 1$ then (Corollary 3 and Corollary 2, i)) $f_k(p,x)$ has at least two different roots in Z_2 and, clearly, one of these must be zero. Then $c_k(p) \equiv 0 \pmod 2$.

THEOREM 9. *For any prime* $k \equiv 5 \pmod 6$, 3 *is a* k-th *power residue of a prime* $p = k.r + 1$ *if and only if* $c_k(p) \equiv 0 \pmod 3$.

Proof. We have seen (Corollary 1') that if $c_k(p) \equiv 0 \pmod 3$ then $(3/p)_k = 1$. Reciprocally, let $(3/p)_k = 1$ and suppose that $c_k(p) \not\equiv 0 \pmod 3$. Then (Corollary 3 and Corollary 2, i)) $f_k(p,x)$ has at least two non-zero different roots in Z_3. Thus,

$$f_k(p,x) \equiv (x - 1)^{n_1} (x - 2)^{n_2} \pmod 3$$

with $0 < n_1 < k$, $0 < n_2 < k$ and $n_1 + n_2 = k$.

Therefore $n_1 + n_2 \equiv k \equiv 2 \pmod 3$ and $n_1 + 2n_2 \equiv -c_1(p) \equiv 2 \pmod 3$ (by (2)). This implies that $n_1 \equiv 2 \pmod 3$ and $n_2 \equiv 0 \pmod 3$. Then, by (3) we have

$$1 \equiv n_1((n_1 - 1)/2) \equiv c_2(p) = -((k - 1)/2).r \equiv r \pmod 3$$

and $p = k.r + 1 \equiv 0 \pmod 3$, which is impossible. Therefore our assumption $c_k(p) \not\equiv 0 \pmod 3$ is false and the theorem is proved.

The preceding proof is not valid for primes $k \equiv 1 \pmod 6$ because in this case $n_1 \equiv 0 \pmod 3$, $n_2 \equiv 1 \pmod 3$, $c_2(p) \equiv 0 \pmod 3$ and the last condition is verified for every r. In a future communication we will consider the validity of Theorem 9 for primes $k \equiv 1 \pmod 6$ and other related results.

REFERENCES

[1] E. E. KUMMER, *Uber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung enstehen*, Journal der Mathematik, vol. 30 (1846), pp. 107-116.

[2] E. LEHMER, *The quintic character of 2 and 3*, Duke Mathematical Journal, vol. 18 (1951), pp. 11-18.

[3] ---------, *Criteria for cubic and quartic residuacity*, Mathematika, vol. 5 (1958), pp. 20-29.

[4] ---------, *On the divisors of the discriminant of the period equation*, American Journal of Mathematics, vol. 90 (1968), pp. 375-379.

[5] J. J. SYLVESTER, *Instantaneous proof of a theorem of Lagrange on the divisors of the form* $Ax^2 + By^2 + Cz^2$ *with a postcript on the divisors of the functions which multisect the primitive roots of unity*, American Journal of Mathematics, vol. 3 (1880), pp. 390-392.

Universidad del Zulia
Maracaibo, Venezuela

Recibido en junio de 1976.