Stanislav Jakubec
Note on the cubic residues


Persistent URL: [http://dml.cz/dmlcz/120514](http://dml.cz/dmlcz/120514)

**Terms of use:**

© University of Ostrava, 1997

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use.*
Note on the Cubic Residues

Stanislav Jakubec

Abstract: In this paper, a simple characterization for a prime \( q \) to be a cubic residue modulo \( p \) is given. This criterion (Corollary 1) is a corollary of Theorem 1, where the decomposition of primes \( q \) onto prime ideals in a cubic subfield of the field \( \mathbb{Q}(\zeta_p) \) is described.

Mathematics Subject Classification: Primary 11R18.

Let \( p \) be a prime, \( p \equiv 1 \pmod{3} \) and let \( K \) be a cubic subfield of the field \( \mathbb{Q}(\zeta_p) \).

**Theorem 1.** Let \( q \) be a prime, \( q \neq 3, q \neq p \), such that it decomposes onto \( r \) prime ideals in \( \mathbb{Z}_{\mathbb{Q}(\zeta_p)} \), where \( 3 \mid r \). Then \( q \) decomposes onto 3 prime ideals in \( \mathbb{Z}_K \).

**Proof.** Then we have two possibilities. Either \( q \) decomposes in \( \mathbb{Z}_K \) onto 3 prime ideals, or \( q\mathbb{Z}_K \) is a prime ideal.

(i) Let \( p \not\equiv 1 \pmod{9} \). Then 3 does not divide \( \frac{p-1}{3} \). Let \( q\mathbb{Z}_K \) be a prime ideal in \( \mathbb{Z}_K \). Then \( \mathbb{Z}_K \) decomposes onto \( r \) prime ideals in \( \mathbb{Z}_{\mathbb{Q}(\zeta_p)} \), hence \( r \mid \frac{p-1}{3} \) - a contradiction.

(ii) Let \( p \equiv 1 \pmod{9} \). Suppose that \( q\mathbb{Z}_K \) is a prime ideal. Let \( \beta_0, \beta_1, \beta_2 \) are Gauss periods. As it is well known (see [1]) \( 1 + 3\beta_0 \) is a root of the polynomial \( f(X) = X^3 - 3pX - (2A - B)p \), where

\[
J(\chi, \chi) = A + B\zeta_3 \equiv -1 \pmod{3}
\]

is the Jacobi sum.

Because \( q\mathbb{Z}_K \) is a prime ideal, we have

\[
[Z_K/q\mathbb{Z}_K : \mathbb{Z}/q\mathbb{Z}] = 3,
\]

Therefore \( f(X) \) is irreducible modulo \( q \) (\( q \neq 3 \)). From the fact that \( q \) decomposes onto \( r \) prime ideals in \( \mathbb{Z}_{\mathbb{Q}(\zeta_p)} \), using the theorem on the degree of the residue field, we get

\[
q^{r-1} \equiv 1 \pmod{p},
\]

hence \( q \) is a cubic residue modulo \( p \).
Let \( H^*(Q(\zeta_3)) \) be the group of ray classes in the narrow sense \((\text{mod } 9)qZ_{Q(\zeta_3)}\).

By [4] Corollary 7 p. 358 there holds: In every class of \( H^*(K) \) there are infinitely many prime ideals, even of the first degree. Consider the class generated by the ideal

\[(*) \quad (A + 3q + (B + 3q)\zeta_3)Z_{Q(\zeta_3)}.

From the fact that \( Z_{Q(\zeta_3)} \) is a ring of principal ideals it follows that the class generated by the ideal \((*)\) consists of ideals of the form \((A' + B'\zeta_3)Z_{Q(\zeta_3)}\), where \(A' \equiv A + 3q \pmod{9q}\) and \(B' \equiv B + 3q \pmod{9q}\). Let \((A^* + B^*\zeta_3)Z_{Q(\zeta_3)}\) be a prime ideal from this class. Let


Because \(B \equiv 0 \pmod{3}\) we have

\[p^* \equiv 1 + 3qA \equiv 1 - 3q \pmod{9},

hence \(p^* \not\equiv 1 \pmod{9}\).

From \(A^* + B^*\zeta_3 \equiv -1 \pmod{3}\) we get that \(A^* + B^*\zeta_3\) is the Jacobi sum for the Dirichlet character modulo \(p^*\). By Lemma 2 of [3] and from the facts that \(A^* + B^*\zeta_3\) is the Jacobi sum, \(q\) is a cubic residue modulo \(p\), and \(A^* + B^*\zeta_3 \equiv A + B\zeta_3 \pmod{q}\), it follows that \(q\) is a cubic residue modulo \(p^*\).

Denote by \(\beta_q^3\) the Gauss period for a prime \(p^*\). Hence \(1 + 3\beta_q^3\) is a root of the polynomial \(f^*(X)\) where \(f^*(X) \equiv f(X) \pmod{q}\) therefore \(f^*(X)\) is irreducible modulo \(q\). By (i) of this proof, \(q\) decomposes onto 3 prime ideals in \(Z_K\) (because \(p^* \not\equiv 1 \pmod{9}\) and \(q\) is a cubic residue modulo \(p^*\)), hence \(f^*(X)\) decomposes modulo \(q\) onto linear factors - a contradiction.

**Corollary 1.** Let \(p \equiv 1 \pmod{3}\), \(4p = a^2 + 27b^2\), \(a \equiv 1 \pmod{3}\). A prime \(q\), \(q \not\equiv 3\) is a cubic residue modulo \(p\) if and only if the polynomial \(f(X) = X^3 - 3pX - ap\) has a root modulo \(q\).

**Proof.** The assertion of this corollary follows from the Theorem 1, if we take into consideration that this polynomial is either irreducible or decomposes onto linear factors, depending on whether \(qZ_K\) is a prime ideal or decomposes on 3 ideals respectively.

**Example 1.** Let \(q\) be a prime \(q \not\equiv 3\). If \(q|ab\), then \(q\) is a cubic residue modulo \(p\).

**Proof.** 1. If \(q|a\), then \(f(X)\) has a root \(X = 0 \pmod{q}\).

2. If \(q|b\), then \(f(X)\) has a root \(X = a \pmod{q}\).
Example 2. If \( q = 2, 5, 7 \), then \( q \) is a cubic residue modulo \( p \) if and only if \( q | ab \).

Proof. If \( q | ab \) then by Example 1 \( q \) is a cubic residue modulo \( p \). Investigating a few possibilities we find that \( f(X) \) is otherwise irreducible.

Remark 1. Theorem 1 and hence Corollary 1, too, can be extended to the case \( q = 3 \). But we must consider the polynomial \( g(X) = X^3 + X^2 - \frac{p-1}{3} X - \frac{aq+3p-1}{27} \), which has the Gauss period \( \beta_0 \) as a root. Let \( g(X) \) decomposes onto linear factor modulo \( 3 \). This decomposition cannot be of the form

\[
g(X) \equiv X(X - 1)(X - 2) \pmod{3},
\]

because \( 0 + 1 + 2 \not\equiv -1 \pmod{3} \). Therefore \( g(X) \) has a multiple root modulo \( 3 \), hence \( 3 | \Lambda \), where \( \Lambda = p^7b^2 \) is a discriminant of the polynomial \( g(X) \). It follows that \( 3 | b \). Conversely if \( 3 | b \) then the polynomial \( g(X) \) has a root modulo \( 3 \). Therefore \( 3 \) is a cubic residue modulo \( p \) if and only if \( 4p = a^2 + 243b^2 \). Because it is consistent with the condition for \( 3 \) to be a cubic residue modulo \( p \) (see [2]), it is a proof of Theorem 1 for \( q = 3 \).

References


