A NOTE ON RESIDUACITY AND CRITERIA FOR PRIME REPRESENTATION

RICHARD A. MOLLIN and ANITHA SRINIVASAN

Department of Mathematics and Statistics
University of Calgary
Canada
e-mail: ramollin@math.ucalgary.ca

Department of Mathematics
Siddhartha College
Affiliated with Mumbai University
India
e-mail: rsrinivasan.anitha@gmail.com

Abstract

We provide a new criterion for the fundamental unit, having norm $-1$, of a real quadratic order to be a quadratic residue modulo a given prime $p$ and relate it to results in the literature that are more easily obtained with our approach.

1. Introduction, Notation and Preliminaries

We will be discussing real quadratic orders the details and background of which may be found in [3, Section 1.5]. If $D_0 > 1$ is a square-free integer, then a fundamental discriminant with fundamental radicand $D_0$ is given by

$$\Delta_0 = \begin{cases} D_0, & \text{if } D_0 \equiv 1 \pmod{4}, \\ 4D_0, & \text{if } D_0 \equiv 2, 3 \pmod{4}. \end{cases}$$

2010 Mathematics Subject Classification: Primary 11R09, 11A55; Secondary 11R11, 11R29.

Keywords and phrases: Pell’s equation, real quadratic fields, continued fractions.

Received February 23, 2010
Now suppose that $\Delta = f_\Delta^2 \Delta_0$ for given positive integer $f_\Delta$. If we set
\[
\sigma_0 = \begin{cases} 2, & \text{if } \Delta_0 \equiv 1 \pmod{4}, \\ 1, & \text{if } \Delta_0 \equiv 0 \pmod{4}, \end{cases}
\]
then for $g = \gcd(\sigma_0, f_\Delta)$, and $\sigma = \sigma_0/g$, $\Delta = 4D/\sigma^2$ is called a discriminant with associated radicand $D = (f/g)2D_0$ (and underlying fundamental discriminant $\Delta_0$ having fundamental radicand $D_0$). Set
\[
\omega_{\Delta_0} = \begin{cases} (1 + \sqrt{D_0})/2, & \text{if } \Delta_0 \equiv 1 \pmod{4}, \\ \sqrt{D_0}, & \text{if } \Delta_0 \equiv 0 \pmod{4}, \end{cases}
\]
then $\omega_\Delta = f_\Delta \omega_{\Delta_0} + h$, where $h \in \mathbb{Z}$ is called the principal surd associated with the discriminant $\Delta$. Thus, if $\omega_\Delta'$ is the algebraic conjugate of $\omega_\Delta$, then $\Delta = (\omega_\Delta - \omega_\Delta')^2$, and $\mathcal{O}_\Delta = [1, f_\Delta \omega_{\Delta_0}] = [1, \omega_\Delta] = \mathbb{Z} + \omega_\Delta \mathbb{Z}$ is called an order in $\mathbb{Q}(\sqrt{D_0})$ having conductor $f_\Delta$ with discriminant $\Delta$ and associated radicand $D$.

The fundamental unit $\varepsilon_\Delta$ of the order $\mathcal{O}_\Delta$ is that unit $\varepsilon_\Delta > 1$ such that any unit $u \in \mathcal{O}_\Delta$ is given by $u = \varepsilon_\Delta^n$ for some $n \in \mathbb{Z}$. When we speak of $\varepsilon_\Delta$ being a (nonzero) quadratic residue modulo a given prime $p$, denoted by the generalized Legendre symbol $(\varepsilon_\Delta/p) = 1$, we mean that $\varepsilon_\Delta$ is a square in $\mathbb{Z}[\sqrt{D}]$.

Also, when we refer to the least positive solution $(x, y) = (A_0, B_0)$ of the Pell equation $x^2 - Dy^2 = -1$, we mean that $A_0 > 0$ and $B_0 > 0$ have least value. This is well defined since it may be shown that if $a + b\sqrt{D}$ and $e + f\sqrt{D}$ are both positive solutions of $x^2 - Dy^2 = c$, for any nonzero $c \in \mathbb{Z}$, then the following are equivalent: (1) $a < e$, (2) $b < f$, (3) $a + b\sqrt{D} < e + f\sqrt{D}$ — see [4] for verification and a generalization of this to solutions of the Diophantine equation $d_1 x^2 - d_2 y^2 = \pm 1$.

2. Prime Representation and Residuacity

In [5], we proved the following:

**Theorem 2.1.** Let $\Delta > 1$ be a discriminant having radicand $D$ with $(D/p) = 1$. \[ \text{ } \]
If \( p \equiv 1 \pmod{4} \) is prime with representation \( p = a^2 + 4b^2 \), and \( x^2 - Dy^2 = -1 \) is solvable with least positive solution \( A_0 + B_0\sqrt{D} \), then the Legendre symbol equality holds:

\[
\left( \frac{e_\Delta}{p} \right) = \left( \frac{2^{-1}aA_0 + b}{p} \right).
\]

**Remark 2.1.** In Theorem 2.1, if \( e_\Delta = a_0 + b_0\sqrt{D} \), then \( 2a_0, 2b_0 \in \mathbb{Z} \), and \((A_0, B_0) \neq (a_0, b_0)\) occurs only if \( D \equiv 5 \pmod{8} \) and \( f_\Delta \) is odd. The converse does not hold as evidenced by \( D = \Delta = 37 = 5 \pmod{8} \) with \( f_\Delta = 1 \) and \((a_0, b_0) = (A_0, B_0) = (6, 1)\). If \((A_0, B_0) \neq (a_0, b_0)\), then \((A_0, B_0) = (a_0^3 + 3a_0b_0^2D, 3a_0^2b_0 + b_0^3D)\) – see [3, Theorem 2.1.4, p. 53] for a proof of these facts.

We begin with a new result for general Kronecker symbols that will lead to a new criterion, Theorem 2.2, for quadratic residuacity expressed in terms of \( D \) rather than \( p \) as in Theorem 2.1.

**Lemma 2.1.** Let \( n \in \mathbb{N} \) be odd with \( n = a^2 + 4b^2 \). Then the Kronecker symbol equality holds for any integer \( A \):

\[
\left( \frac{aA + b}{n} \right) = \left( \frac{aA + b}{4A^2 + 1} \right).
\]

**Proof.** We have, observing that if \( aA + b \) is even, then \((2/n) = (n/2)\) given that \( n \equiv 1 \pmod{4} \):

\[
\left( \frac{aA + b}{n} \right) = \left( \frac{n}{aA + b} \right) = \left( \frac{a^2 + 4b^2}{aA + b} \right) = \left( \frac{(2Aa + 2b)^2 - a^2(4A^2 - 1) - 8Aab}{aA + b} \right) = \left( \frac{-a^2(4A^2 - 1) - 8Aab}{aA + b} \right).
\]

\[
= \left( \frac{-a}{aA + b} \right) \cdot \left( \frac{a(4A^2 - 1) + 8Ab}{aA + b} \right) = \left( \frac{-a}{aA + b} \right) \cdot \left( \frac{4A(aA + b) - a + 4bA}{aA + b} \right).
\]
\[
\frac{-a}{aA + b} \cdot \left(\frac{-a + 4bA}{aA + b}\right) = \left(\frac{-a}{aA + b}\right) \left(\frac{a}{aA + b}\right) \left(\frac{-1 + 4a^{-1}bA}{aA + b}\right) = \left(\frac{-1}{aA + b}\right) \left(\frac{-1 - 4A^2}{aA + b}\right) = \left(\frac{4A^2 + 1}{aA + b}\right) = \left(\frac{aA + b}{4A^2 + 1}\right),
\]
which is the result.

**Theorem 2.2.** Let \( \Delta > 1 \) be a discriminant with radicand \( D \). Suppose that \( p = a^2 + 4b^2 \) is prime and \( A_0 + B_0\sqrt{D} \) is the least positive solution of \( x^2 - Dy^2 = -1 \) with the Legendre symbol equality \( (D/p) = 1 \). Then the Kronecker symbol equality holds:

\[
\left(\frac{\varepsilon_\Delta}{p}\right) = \left(\frac{2^{-1}aA_0 + b}{D}\right),
\]

where \( 2^{-1} \) is taken modulo \( p \) and \( \varepsilon_\Delta \) is the fundamental unit of the order \( \mathcal{O}_\Delta \).

**Proof.** By Theorem 2.1,

\[
\left(\frac{\varepsilon_\Delta}{p}\right) = \left(\frac{2^{-1}aA_0 + b}{p}\right),
\]

so by letting \( A = A_0 2^{-1} \) in Lemma 2.1, we get the result.

**Example 2.1.** Let \( p = 13 = 3^2 + 4 \cdot 1^2 = a^2 + 4b^2, \Delta = 4D = 4 \cdot 53 \), for which \( A_0 = 182, B_0 = 25 \). Then

\[
\left(\frac{\varepsilon_\Delta}{p}\right) = \left(\frac{182 + 25\sqrt{53}}{53}\right) = 1
\]
since \( 182 + 25\sqrt{53} \equiv (2 + 3\sqrt{53})^2 \pmod{13} \), and indeed

\[
\left(\frac{2^{-1}aA_0 + b}{D}\right) = \left(\frac{2^{-1}aA_0 + b}{53}\right) = \left(\frac{27 \cdot 3 \cdot 182 + 1}{53}\right) = 1,
\]
as predicted by Theorem 2.2. On the other hand, if \( \Delta = 4D = 4 \cdot 29 \), then \( A_0 = 70, B_0 = 13 \),

\[
\left(\frac{2^{-1}aA_0 + b}{D}\right) = \left(\frac{2^{-1}aA_0 + b}{29}\right) = \left(\frac{21 \cdot 3 \cdot 70 + 1}{29}\right) = -1,
\]
and \( 70 + 113\sqrt{29} \neq x^2 \pmod{13} \) for any non-zero \( x \), as told by Theorem 2.2.

**Corollary 2.1.** Let \( p = a^2 + 4b^2, \quad q = 1 \pmod{4} \) be primes with \( (p/q) = (q/p) = 1 \), and \( A_0 + B_0\sqrt{q} \) the least positive solution of \( x^2 - qy^2 = -1 \). Then

\[
\left( \frac{q}{p} \right)_4 \left( \frac{p}{q} \right)_4 = \left( \frac{2^{-1}aA_0 + b}{q} \right).
\]

**Proof.** By Scholz [6], the left-hand side equals \( (\varepsilon_q/p) \) and by Theorem 2.2 that equals the right-hand side.

**Example 2.2.** Let \( p = 5 = 1^2 + 4 \cdot 1^2 = a^2 + 4b^2 \) and \( q = 29 \), for which \( A_0 + B_0\sqrt{q} = 70 + 12\sqrt{29} \). Then

\[
\left( \frac{2^{-1}aA_0 + b}{q} \right) = \left( \frac{1051}{4901} \right) = 1.
\]

Also \( \left( \frac{5}{29} \right)_4 \left( \frac{29}{5} \right)_4 = 1 \) since \( \left( \frac{5}{29} \right)_4 = -1 = \left( \frac{29}{5} \right)_4 \).

**Corollary 2.2.** If \( p = a^2 + 4b^2 \) and \( q = c^2 + 4d^2 \) are primes with \( (p/q) = (q/p) = 1 \) and \( A_0 + B_0\sqrt{q} \) is the least positive solution of \( x^2 - qy^2 = -1 \), then the Kronecker symbol equality holds:

\[
\left( \frac{2^{-1}aA_0 + b}{p} \right) = (-1)^{(p-1)/4} \left( \frac{2ad - 2bc}{p} \right).
\]

**Proof.** By Corollary 2.1, \( (p/q)_4(q/p)_4 \) equals the left hand side and by Burde [2] it equals the right hand side.

**Example 2.3.** Let \( p = 17 = 1^2 + 4 \cdot 2^2 = a^2 + 4b^2, \quad q = 13 = 3^2 + 4 \cdot 1^2 = c^2 + 4d^2 \), for which \( A_0 + B_0\sqrt{p} = 4 + \sqrt{17} \). Then

\[
\left( \frac{2^{-1}aA_0 + b}{p} \right) = \left( \frac{p}{2^{-1}aA_0 + b} \right) = \left( \frac{17}{109} \right) = -1
\]

\[
= (-1)^{(17-1)/4} \left( \frac{10}{17} \right) = (-1)^{(p-1)/4} \left( \frac{2ad - 2bc}{p} \right).
\]
Theorem 2.3. A prime \( p \equiv 1 \pmod{20} \) is represented by both or neither of
\( f(x, y) = x^2 + 20y^2 \) and \( g(x, y) = x^2 + 100y^2 \). A prime \( p \equiv 9 \pmod{20} \) is
represented by exactly one of \( f \) or \( g \).

Proof. If \( p = a^2 + 4b^2 \) is represented by \( f \), then by [7, Remark 6.1, p. 38],
\( (\varepsilon_5/p) = 1 \) and so by Theorem 2.2,
\[
\left( \frac{5}{a+b} \right) = 1
\]
(2.1)
since \( A_0 = 2 \) and \( B_0 = 1 \) with \( \varepsilon_D = \varepsilon_5 = (1 + \sqrt{5})/2 \) and \( \varepsilon_D^3 = A_0 + B_0\sqrt{D} = 2 + \sqrt{5} \). If \( p \) is not represented by \( f \), then it is represented by \( 4x^2 + 5y^2 \) the other
form in the principal genus of discriminant \(-4 \cdot 20\), so we have in either case \( p \equiv \pm 1 \pmod{5} \).

Case 2.1. \( p \) is represented by \( g \).

In this case, \( a = x \) and \( b = 5y \), so by (2.1), if \( p \) is represented by \( f \), then
\( (x/5) = 1 \) so \( p = x^2 = 1 \pmod{20} \). If \( p \) is not represented by \( f \), then \( (x/5) = -1 \) so
\( p = x^2 = 9 \pmod{20} \).

Case 2.2. \( p \) is not represented by \( g \).

In this case, \( b \not\equiv 0 \pmod{5} \) and \( p \equiv a^2 - b^2 \pmod{5} \). Also \( p \equiv \pm 1 \pmod{5} \)
so we must have \( a \equiv 0 \pmod{5} \). Thus by (2.1), if \( p \) is represented by \( f \), then
\( (b/5) = 1 \) which means that \( b \equiv \pm 1 \pmod{5} \) so \( b^2 \equiv 1 \pmod{5} \) and \( p \equiv a^2 - b^2 \equiv -1 \pmod{5} \). If \( p \) is not represented by \( f \), then \( (b/5) = -1 \) so \( b \equiv 2, 3 \pmod{5} \) and
\( b^2 \equiv -1 \pmod{5} \) so \( p \equiv a^2 - b^2 \equiv 1 \pmod{5} \).

Remark 2.2. Theorem 2.3 appears as [1, Theorem 1, p. 465], where there are five “peculiar theorems” presented but our proof is much more elementary and shows the interplay among genus theory, residuacity, and prime representation.

Acknowledgement

The first author gratefully acknowledges the support of NSERC Canada grant # A8484.
References


