<table>
<thead>
<tr>
<th>Title</th>
<th>Note on certain quadratic nonresidues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Washio, Tadashi; Kodama, Tetsuo</td>
</tr>
<tr>
<td>Citation</td>
<td>長崎大学教育学部紀要 [自然科学] 長崎大学教育学部紀要</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2005-03-28</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10069/6138">http://hdl.handle.net/10069/6138</a></td>
</tr>
</tbody>
</table>

NAOSITE: Nagasaki University’s Academic Output SITE

http://naosite.lb.nagasaki-u.ac.jp
Note on certain quadratic nonresidues

Tadashi WASHIO and Tetsuo KODAMA*

Department of Mathematics, Faculty of Education, Nagasaki University, Nagasaki 852, Japan
(Received October 29, 2004)

Abstract
This note is devoted to studying quadratic nonresidues attached to certain binary representations of prime numbers and quadratic nonresidues derived from certain quadratic congruences.

1. Introduction

Let \( p \) be a prime number. In the case of considering a quadratic congruence equation modulo \( p \), it has no solution if and only if its discriminant is a quadratic nonresidue modulo \( p \). It is well-known that there are some typical examples of quadratic nonresidues. For instance, the first complementary law tells us that \((-1/p) = -1\) if and only if \( p \equiv 3 \pmod{4} \) and the second complementary law shows that \((2/p) = -1\) if and only if \( p \equiv \pm 3 \pmod{8} \), where \((\bullet/p)\) means the Legendre symbol. Moreover \((3/p) = -1\) if and only if \( p \equiv \pm 5 \pmod{12} \) and \((5/p) = -1\) if and only if \( p \equiv \pm 2 \pmod{5} \), (see Takagi[2]). In this note we want to study quadratic nonresidues attached to certain binary representations of prime numbers and quadratic nonresidues derived from certain quadratic congruences.

2. Quadratic nonresidues attached to the binary forms of prime numbers

As is well-known, prime numbers of some kind have the expression of binary quadratic forms. For instance, if a prime number \( p \) is congruent to 9 modulo 16 then there exist integers \( a \) and \( b \) satisfying

\[
p = a^2 - 2b^2,
\]

*Professor emeritus, Kyushu University, Fukuoka 812, Japan.
and a prime number \( p \) is congruent to 13 modulo 24 then there exist integers \( a \) and \( b \) satisfying
\[
p = a^2 - 3b^2,
\]
(see Hasse [1] and Takagi [2]).

In this section we study quadratic nonresidues attached to such binary quadratic expressions of those prime numbers. We start with the following lemma.

**Lemma 1.** Let \( p \) be a prime number and \( c \) an integer. If \( p \equiv 9 \pmod{16} \) and \( c^2 \equiv 2 \pmod{p} \) then \( 2 \pm c \) are quadratic nonresidues modulo \( p \).

**Proof.** Let \( u \) be a primitive root modulo \( p \) and put \( v = u^m \) where \( m = (p - 1)/8 \). Then it is clear that \( m \) is an odd integer and so that \( v \) is a quadratic nonresidue modulo \( p \). Since \( v^4 \equiv -1 \pmod{p} \), we have
\[
(1 + v^2)^2 \equiv 2v^2 \equiv c^2v^2 \pmod{p}.
\]

Multiplying by \(-v^2\) to both sides yields
\[
c^2 \equiv -v^2(1 + v^2)^2 \equiv v^6(1 + v^2)^2 \pmod{p}.
\]

Therefore we get
\[
2 \pm c \equiv c^2 \pm c \equiv v^6(1 + v^2)^2 \pm v^3(1 + v^2) \pmod{p}
\]
\[
\equiv v^3\{2v^5 \pm (1 + v^2)\} \equiv \pm v^3(1 \mp v)^2 \pmod{p}.
\]

Hence the desired assertion follows at once from the fact that \( v \) is a quadratic nonresidue modulo \( p \).

**Theorem 2.** Let \( p \) be a prime number and \( a \) and \( b \) integers.

(1) If \( p \equiv 9 \pmod{16} \) and \( p = a^2 - 2b^2 \) then \( a(a \pm b) \) are quadratic nonresidues modulo \( p \).

(2) If \( p \equiv 13 \pmod{24} \) and \( p = a^2 - 3b^2 \) then \( b(2b \pm a) \) are quadratic nonresidues modulo \( p \).
Note on certain quadratic nonresidues

PROOF. (1) Because of \( p \equiv 9 \pmod{16} \), we can take an integer \( c \) satisfying \( c^2 \equiv 2 \pmod{p} \). Then, \( a^2 \equiv b^2 c^2 \pmod{p} \), we obtain \( a \equiv \pm bc \pmod{p} \). This leads that

\[
a(a \pm b) \equiv b^2 c^2 \pm b^2 c \equiv b^2(2 \pm c) \pmod{p}.
\]

Therefore, by using Lemma 1, we have the first assertion.

(2) From \( p = a^2 - 3b^2 \), it is obvious that

\[
2b(2b \pm a) \equiv (a \pm b)^2 \pmod{p}.
\]

Using this and the fact that \( (2/p) = -1 \), we get also the second assertion.

3. Quadratic nonresidual solutions of quadratic congruences

In this section we study quadratic nonresidual solutions of certain quadratic congruence equations.

THEOREM 3. Let \( p \) be an odd prime number and denote by \( r \) an integer satisfying \( 8r \equiv 1 \pmod{p} \).

(1) If \( p \equiv 9 \pmod{16} \) then there exist two distinct solutions modulo \( p \) of the congruence equation

\[
2X^2 - 4rX + r^2 \equiv 0 \pmod{p}.
\]

Such solutions are quadratic nonresidues modulo \( p \).

(2) If \( p \equiv 13 \pmod{24} \) then there exist two distinct solutions modulo \( p \) of the congruence equation

\[
4X^2 - X + r^2 \equiv 0 \pmod{p}.
\]

Such solutions are also quadratic nonresidues modulo \( p \).

PROOF. (1) Because of \( (2/p) = 1 \) the discriminant of \( 2X^2 - 4rX + r^2 \) is equal to \( 8r^2 \) and it is a quadratic residue modulo \( p \). Thus the congruence equation (1) has two distinct solutions \( s \) and \( t \) modulo \( p \). Put \( x = s \) or \( t \) and denote by \( c \) an integer satisfying \( c^2 \equiv 2 \pmod{p} \). Then from (1), we get

\[
(cx + r)^2 \equiv 2crx + 4rx \equiv 2r(2 + c)x \pmod{p}.
\]
Therefore applying Lemma 1 gives us that $x$ is a quadratic nonresidue modulo $p$. This proves the first assertion.

(2) Because of $(2/p) = -1$ and of $(3/p) = 1$ the discriminant of $4X^2 - X + r^2$ is congruent to $6r$ modulo $p$ and it is a quadratic residue modulo $p$. So the congruence equation (2) has two distinct solutions $s$ and $t$ modulo $p$. Put $x = s$ or $t$. Then from (2), we obtain

$$(2x - r)^2 \equiv (1 - 4r)x \equiv 4rx \pmod{p}.$$ 

This leads that $x$ is a quadratic nonresidue modulo $p$. This concludes the proof.

Let $p$ be a prime number. Then the finite prime field $\mathbb{Z}_p$ of characteristic $p$ is identified with the field of residue classes modulo $p$ and so considering polynomials over $\mathbb{Z}_p$ is equivalent to considering congruences with integer coefficients modulo $p$. From this point of view, we can rewrite Theorem 3 as follows.

**Corollary 4.** Let $p$ be an odd prime number and denote by $r$ the element in $\mathbb{Z}_p$ satisfying $8r = 1$.

1. If $p \equiv 9 \pmod{16}$ then there exist two distinct solutions $s$ and $t$ in $\mathbb{Z}_p$ of the equation $X^2 - 2rX + r^2/2 = 0$ and two polynomials $X^2 + X + s$ and $X^2 + X + t$ are irreducible over $\mathbb{Z}_p$.

2. If $p \equiv 13 \pmod{24}$ then there exist two distinct solutions $s$ and $t$ in $\mathbb{Z}_p$ of the equation $X^2 - 2rX + r^2/4 = 0$ and two polynomials $X^2 + X + s$ and $X^2 + X + t$ are irreducible over $\mathbb{Z}_p$.

**Proof.** In Theorem 3, we know the existence of such solutions for above equations and the non-squareness of $s$ and $t$. Moreover, because of $4s + 4t = 1$, the discriminants of our polynomials are $4s$ or $4t$ and so we see the irreducibility of polynomials above.

**References**
