Journal of Number Theory 147 (2015) 694–707

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

New reciprocity laws for octic residues and nonresidues

Zhi-Hong Sun [1]

School of Mathematical Sciences, Huaiyin Normal University, Huaian, Jiangsu 223001, PR China

A R T I C L E   I N F O

Article history:
Received 9 July 2014
Received in revised form 25 July 2014
Accepted 3 August 2014
Available online 7 October 2014
Communicated by David Goss

MSC:
primary 11A15
secondary 11A07, 11B39, 11E25

Keywords:
Reciprocity law
Octic residue
Congruence
Quartic Jacobi symbol
Lucas sequence

A B S T R A C T

Let $\mathbb{Z}$ be the set of integers, and let p be a prime of the form $8k+1$. Suppose $q \in \mathbb{Z}$, $2 \nmid q$, $p \nmid q$, $p = c^2 + d^2 = x^2 + 2qy^2$, $c, d, x, y \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$. In this paper we establish congruences for $(-q)^{(p-1)/8} \pmod p$ and present new reciprocity laws.

E-mail address: zhihongsun@yahoo.com.
URL: http://www.hytc.edu.cn/xsjl/szh.

[1] Supported by the National Natural Science Foundation of China (grant No. 11371163).

http://dx.doi.org/10.1016/j.jnt.2014.08.015
0022-314X/

1. Introduction

Let $\mathbb{Z}$ be the set of integers, $i = \sqrt{-1}$ and $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. For any positive odd number m and $a \in \mathbb{Z}$ let $(\frac{a}{m})$ be the (quadratic) Jacobi symbol. For convenience we also define $(\frac{a}{1}) = 1$ and $(\frac{a}{-m}) = (\frac{a}{m})$. Then for any two odd numbers m and n with $m > 0$ or $n > 0$ we have the following general quadratic reciprocity law: $(\frac{m}{n}) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}(\frac{n}{m})$.

For $a, b, c, d \in \mathbb{Z}$ with $2 \nmid c$ and $2 \mid d$, one can define the quartic Jacobi symbol $(\frac{a+bi}{c+di})_4$ as in [S1,S2,S4]. From [IR] we know that $(\frac{a-bi}{c-di})_4 = (\frac{a+bi}{c+di})_4^{-1}$. In Section 2 we list main properties of the quartic Jacobi symbol. See also [IR,BEW,S4]. For the history of quartic reciprocity laws, see [Lem].

Let p be a prime of the form $4k + 1$, $q \in \mathbb{Z}$, $2 \nmid q$ and $p \nmid q$. Suppose that $p = c^2 + d^2 = x^2 + qy^2$, $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume that $(c, x + d) = 1$ or $(d_0, x + c) = 1$, where (m, n) is the greatest common divisor of m and n. In [S5], using the quartic reciprocity law the author deduced some congruences for $q^{[p/8]} \pmod p$ in terms of c, d, x and y, where $[a]$ is the greatest integer not exceeding a.

Let p be a prime of the form $8k+1$, $q \in \mathbb{Z}$, $2 \nmid q$ and $p \nmid q$. Then q is an octic residue $\pmod p$ if and only if $q^{(p-1)/8} \equiv 1 \pmod p$. In the classical octic reciprocity laws (see [Lem] and [BEW]), we always assume that $p = c^2 + d^2 = a^2 + 2b^2$ ($a, b, c, d \in \mathbb{Z}$). Inspired by [S5], in this paper we continue to discuss congruences for $(-q)^{(p-1)/8} \pmod p$ and present new reciprocity laws, but we assume that $p = c^2 + d^2 = x^2 + 2qy^2$. Here are some typical results:

- ⋆ Let p and q be primes such that $p \equiv 1 \pmod 8$, $q \equiv 7 \pmod 8$, $p = c^2+d^2 = x^2+2qy^2$, $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$. Then $(-q)^{\frac{p-1}{8}} \equiv (\frac{d}{c})^m \pmod p$ if and only if $(\frac{c-di}{c+di})^{\frac{q+1}{8}} \equiv i^m \pmod q$.
- ⋆ Let $p \equiv 1 \pmod 8$ be a prime, $p = c^2 + d^2 = x^2 + 2(a^2 + b^2)y^2$, $a, b, c, d, x, y \in \mathbb{Z}$, $a \neq 0$, $4 \mid a$, $(a, b) = 1$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then $(-a^2-b^2)^{\frac{p-1}{8}} \equiv (-1)^{\frac{d}{4}+\frac{y}{2}}(\frac{c}{d})^m \pmod p$ if and only if $(\frac{(ac+bd)/x}{b+ai})_4 = i^m$.
- ⋆ Let p be a prime of the form $8k+1$ and $a \in \mathbb{Z}$ with $2 \nmid a$. Suppose that $p = c^2+d^2 = x^2 + (a^2 + 1)y^2$, $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0 (2 \nmid d_0)$ and $4 \mid y$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$. Then $(a + \sqrt{a^2+1})^{\frac{p-1}{4}} \equiv (-1)^{\frac{d}{4}+\frac{y}{4}} \pmod p$.

When a is even, a congruence for $(a + \sqrt{a^2+1})^{(p-1)/4} \pmod p$ was given by the author in [S6, Corollary 4.1]. When $a \geq 3$ is a positive integer and $a^2 + 1$ is squarefree, $a + \sqrt{a^2+1}$ is just the fundamental unit ε_{a^2+1} of the quadratic field $\mathbb{Q}(\sqrt{a^2+1})$. For early results and conjectures on $\varepsilon_d^{(p-1)/4} \pmod p$, see [L2,LW1,LW2,HK,Lem,S2].

Throughout this paper, if $n \in \mathbb{Z}$, $2^\alpha \mid n$ and $2^{\alpha+1} \nmid n$, then we write that $2^\alpha \parallel n$.