CONSECUTIVE NUMBERS WITH THE SAME LEGENDRE SYMBOL

ZHI-HONG SUN

(Communicated by David E. Rohrlich)

ABSTRACT. Let p be an odd prime, and R_p be a complete set of residues (mod p). The goal of the paper is to determine all the values of n ($n \in R_p$) such that $(\frac{n}{p}) = (\frac{n+1}{p})$ or $(\frac{n-1}{p}) = (\frac{n}{p}) = (\frac{n+1}{p})$, where $(\frac{\cdot}{p})$ is the Legendre symbol.

1. INTRODUCTION

Let p be an odd prime, and $(\frac{\cdot}{p})$ be the Legendre symbol, and let R_p be a complete set of residues modulo p . It is well known that (see [D])

$$(1) \quad \left| \left\{ n \mid \left(\frac{n}{p} \right) = \left(\frac{n+1}{p} \right) = 1, \ n \in R_p \right\} \right| = \left[\frac{p-3}{4} \right]$$

and

$$(2) \quad \left| \left\{ n \mid \left(\frac{n}{p} \right) = \left(\frac{n+1}{p} \right) = -1, \ n \in R_p \right\} \right| = \left[\frac{p-1}{4} \right],$$

where $[\cdot]$ is the greatest integer function.

In this paper we construct two or three consecutive numbers with the same value of Legendre symbols by proving the following two theorems.

Theorem 1. *Let p be an odd prime, R_p be a complete set of residues (mod p), and let g be a primitive root of p . Then*

$$\begin{aligned} & \left\{ n \mid \left(\frac{n}{p} \right) = \left(\frac{n+1}{p} \right) = 1, \ n \in R_p \right\} \\ &= \left\{ x_k \mid x_k \equiv \frac{(g^{2k} - 1)^2}{4g^{2k}} \pmod{p}, \ x_k \in R_p, \ k = 1, 2, \dots, \left[\frac{p-3}{4} \right] \right\} \end{aligned}$$

and

$$\begin{aligned} & \left\{ n \mid \left(\frac{n}{p} \right) = \left(\frac{n+1}{p} \right) = -1, \ n \in R_p \right\} \\ &= \left\{ y_k \mid y_k \equiv \frac{(g^{2k-1} - 1)^2}{4g^{2k-1}} \pmod{p}, \ y_k \in R_p, \ k = 1, 2, \dots, \left[\frac{p-1}{4} \right] \right\}. \end{aligned}$$

Received by the editors February 27, 2001.

2000 *Mathematics Subject Classification.* Primary 11A15; Secondary 11A07.

Key words and phrases. Prime, Legendre symbol.

Theorem 2. Let p be an odd prime, $F_p = \mathbb{Z}/p\mathbb{Z}$ be the residue class ring modulo p , and let $F_{p^2} \supset F_p$ be the field with p^2 elements. If g is a generator of the cyclic subgroup of $F_{p^2}^*$ ($= F_{p^2} - \{0\}$) of order $p - (\frac{-1}{p})$, then

$$\left\{ n \mid \left(\frac{n-1}{p} \right) = \left(\frac{n}{p} \right) = \left(\frac{n+1}{p} \right), n \in F_p \right\} \\ = \left\{ \pm \frac{2g^{\frac{p-(\frac{-1}{p})}{4}+2s}}{g^{4s}-1} \mid s = 1, 2, \dots, \left[\frac{p-3}{8} \right] \right\}.$$

We remark that if $p \equiv 1 \pmod{4}$, then g is a primitive root $\pmod{p}$, and if $p \equiv 3 \pmod{4}$ we may take $F_{p^2} = \{a + bi \mid a, b \in F_p\}$ and write $g = a + bi$ with $a, b \in F_p$ and $a^2 + b^2 = 1$.

In the paper we also establish the following result.

Theorem 3. Let p be an odd prime, and $n \in \mathbb{Z}$ with $n \not\equiv 0, \pm 1 \pmod{p}$. Then

$$\left(\frac{n-1}{p} \right) = \left(\frac{n}{p} \right) = \left(\frac{n+1}{p} \right) \iff n \equiv \frac{(x^2+1)^2}{4x^3-4x} \pmod{p} \quad \text{for some } x \in \mathbb{Z}.$$

Throughout this paper, we denote the set of integers by $\mathbb{Z}$ as usual, and identify $(\frac{a+p\mathbb{Z}}{p})$ with $(\frac{a}{p})$ for $a \in \mathbb{Z}$. For later convenience, we will also denote the Legendre symbol $(\frac{n}{p})$ by $\chi(n)$.

2. PROOF OF THEOREM 1

For $k = 1, 2, \dots, (p-3)/2$ let $m_k \in R_p$ be given by $m_k \equiv (g^k - 1)^2 / (4g^k) \pmod{p}$. Then $m_k + 1 \equiv (g^k + 1)^2 / (4g^k) \pmod{p}$. So $\chi(m_k) = \chi(m_k + 1) = (-1)^k$. If $s, t \in \{1, 2, \dots, \frac{p-3}{2}\}$ with $s \neq t$, then $g^{s+t} \not\equiv 1 \pmod{p}$ and so $g^s - g^t \not\equiv (g^s - g^t)/g^{s+t} \pmod{p}$. This implies that $g^s + g^{-s} \not\equiv g^t + g^{-t} \pmod{p}$ and so $m_s \not\equiv m_t \pmod{p}$. Since

$$\left| \left\{ n \mid \chi(n) = \chi(n+1), n \in R_p \right\} \right| = \left[\frac{p-3}{4} \right] + \left[\frac{p-1}{4} \right] = \frac{p-3}{2}$$

by (1) and (2), we obtain

$$\{n \mid \chi(n) = \chi(n+1), n \in R_p\} = \{m_1, m_2, \dots, m_{\frac{p-3}{2}}\}.$$

This together with the fact that $\chi(m_k) = (-1)^k$ yields the result.

Remark 1. Let $p > 3$ be a prime, and $n \in \mathbb{Z}$ with $p \nmid n(n+1)$. It follows from Theorem 1 that

$$\chi(n) = \chi(n+1) \iff n \equiv \frac{(x-1)^2}{4x} \pmod{p} \quad \text{for some } x \in \mathbb{Z}.$$

Using Theorem 1 one can also derive that

$$\sum_{\substack{\chi(n)=\chi(n+1)=1 \\ n \in R_p}} n \equiv \frac{3+2\chi(-1)}{8} \pmod{p}$$

and

$$\sum_{\substack{\chi(n)=\chi(n+1)=-1 \\ n \in R_p}} n \equiv \frac{3-2\chi(-1)}{8} \pmod{p}.$$

3. PROOF OF THEOREM 2

For $s \in \{1, 2, \dots, [\frac{p-3}{8}]\}$ let $n_s = 2g^{(p-\chi(-1))/4+2s}/(g^{4s}-1)$. Then $n_s \in F_{p^2}$ since $g^{4s} \neq 1$. We claim that $n_s \in F_p$. If $p \equiv 1 \pmod{4}$, then $g^{p-1} = 1$ and so $g^p = g$. Hence $g \in F_p$ and therefore $n_s \in F_p$. If $p \equiv 3 \pmod{4}$, then $g^{p+1} = g^{p-\chi(-1)} = 1$ and hence $g^{-1} = g^p$. So we have

$$g^{\frac{p+1}{4}+2s} + g^{-(\frac{p+1}{4}+2s)} = g^{\frac{p+1}{4}+2s} + (g^{\frac{p+1}{4}+2s})^p = \text{tr}(g^{\frac{p+1}{4}+2s}) \in F_p,$$

where $\text{tr}(\cdot)$ is the trace function. Now, using the above and the fact that $g^{(p+1)/2} = -1$ we see that

$$n_s = -\frac{2}{g^{\frac{p+1}{4}+2s} + g^{-(\frac{p+1}{4}+2s)}} \in F_p.$$

So the assertion holds.

Since $g^{(p-\chi(-1))/2} = -1$ it is easily seen that

$$\begin{aligned} n_s - 1 &= (g^{(p-\chi(-1))/4+2s} + 1)^2 / (g^{4s} - 1), \\ n_s &= (1 + g^{(p-\chi(-1))/4})^2 g^{2s} / (g^{4s} - 1), \\ n_s + 1 &= (g^{(p-\chi(-1))/4} + g^{2s})^2 / (g^{4s} - 1). \end{aligned}$$

From this one can check that

$$\frac{n_s \pm 1}{n_s} = \frac{1}{4} \left(g^s + g^{-s} + g^{\frac{p-\chi(-1)}{4} \mp s} + g^{-(\frac{p-\chi(-1)}{4} \mp s)} \right)^2.$$

If $p \equiv 3 \pmod{4}$, then $g^k + g^{-k} = g^k + g^{kp} = \text{tr}(g^k) \in F_p$. If $p \equiv 1 \pmod{4}$, then $g \in F_p$ and so $g^k + g^{-k} \in F_p$. Thus, by the above we see that $n_s + 1 = n_s x^2$ and $n_s - 1 = n_s y^2$ for some $x, y \in F_p$. Observe that $n_s(n_s - 1)(n_s + 1) \neq 0$ since $1 \leq s \leq (p-3)/8$. Then we have

$$\chi(n_s - 1) = \chi(n_s) = \chi(n_s + 1) \quad \text{and hence} \quad \chi(-n_s - 1) = \chi(-n_s) = \chi(-n_s + 1).$$

If $s, t \in \{1, 2, \dots, [\frac{p-3}{8}]\}$ with $s \neq t$, then clearly $g^{2s-2t}, g^{2s+2t} \neq \pm 1$ and so $g^{2s+2t}(g^{2t} \pm g^{2s}) \neq g^{2s} \pm g^{2t}$. This implies

$$g^{2s}(g^{4t} - 1) \neq \pm g^{2t}(g^{4s} - 1) \quad \text{and hence} \quad \frac{g^{2s}}{g^{4s} - 1} \neq \pm \frac{g^{2t}}{g^{4t} - 1}.$$

Thus $n_s \neq \pm n_t$.

According to [BEW] or [D], if $b, c \in \mathbb{Z}$ with $b^2 - 4c \not\equiv 0 \pmod{p}$, then

$$(3) \quad \sum_{n=0}^{p-1} \chi(n^2 + bn + c) = -1.$$

Set

$$(4) \quad R = |\{n \mid \chi(n-1) = \chi(n) = \chi(n+1) = 1, n \in F_p\}|$$

and

$$(5) \quad N = |\{n \mid \chi(n-1) = \chi(n) = \chi(n+1) = -1, n \in F_p\}|.$$

Then we see that

$$(6) \quad \sum_{n=2}^{p-2} (1 + \chi(n-1))(1 + \chi(n))(1 + \chi(n+1)) = 8R$$

and

$$\sum_{n=2}^{p-2} (1 - \chi(n-1))(1 - \chi(n))(1 - \chi(n+1)) = 8N.$$

So, by (3) we have

$$\begin{aligned} 8(R + N) &= \sum_{n=2}^{p-2} \{ (1 + \chi(n-1))(1 + \chi(n))(1 + \chi(n+1)) \\ &\quad + (1 - \chi(n-1))(1 - \chi(n))(1 - \chi(n+1)) \} \\ &= 2 \sum_{n=2}^{p-2} \{ 1 + \chi(n^2 - n) + \chi(n^2 + n) + \chi(n^2 - 1) \} \\ &= 2(p-3) + 2 \left\{ \sum_{n=0}^{p-1} (\chi(n^2 - n) + \chi(n^2 + n) + \chi(n^2 - 1)) - 2\chi(2) - \chi(-1) \right\} \\ &= 2(p-3) - 6 - 4\chi(2) - 2\chi(-1) = 16 \left[\frac{p-3}{8} \right]. \end{aligned}$$

That is,

$$R + N = 2 \left[\frac{p-3}{8} \right].$$

Now, combining the above we prove the theorem.

Remark 2. Let $p \equiv 1 \pmod{4}$ be a prime, $p = a^2 + b^2$ ($a, b \in \mathbb{Z}$), $a \equiv 1 \pmod{4}$, and g be a primitive root of p . If R and N are defined by (4) and (5) respectively, using (3), (6) and the fact that $\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) = 0$ and $\sum_{n=0}^{p-1} \left(\frac{n^3-n}{p}\right) = -2\left(\frac{2}{p}\right)a$ (cf. [J], [BE, Theorem 4.4]) we see that

$$\begin{aligned} R &= \frac{1}{8} \sum_{n=0}^{p-1} (1 + \chi(n-1))(1 + \chi(n))(1 + \chi(n+1)) - 1 - \frac{1}{2}\chi(2) \\ &= \frac{1}{8} \left\{ p + \sum_{n=0}^{p-1} (\chi(n^2 - n) + \chi(n^2 + n) + \chi(n^2 - 1) + \chi(n^3 - n)) \right\} - 1 - \frac{1}{2}\chi(2) \\ &= \frac{1}{8} (p - 3 - 2\chi(2)a) - 1 - \frac{1}{2}\chi(2) \\ &= \begin{cases} \frac{p-17}{8} - \frac{a-1}{4} & \text{if } p \equiv 1 \pmod{8}, \\ \frac{p-5}{8} + \frac{a-1}{4} & \text{if } p \equiv 5 \pmod{8} \end{cases} \end{aligned}$$

and therefore

$$N = 2 \left[\frac{p-3}{8} \right] - R = \begin{cases} \frac{p-1}{8} + \frac{a-1}{4} & \text{if } p \equiv 1 \pmod{8}, \\ \frac{p-5}{8} - \frac{a-1}{4} & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

4. PROOF OF THEOREM 3

Let $Q_0(p)$ be defined as in [S]. From [S, Theorem 2.4] and [S, Corollary 3.2] we see that

$$\begin{aligned} \left(\frac{n-1}{p}\right) = \left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right) &\iff n^2 \equiv k^2 + 1 \pmod{p} \quad \text{for some } k \in Q_0(p) \\ &\iff n^2 \equiv \left(\frac{x^4 - 6x^2 + 1}{4x^3 - 4x}\right)^2 + 1 \pmod{p} \quad \text{for some } x \in \mathbb{Z} \\ &\iff n^2 \equiv \frac{(x^2 + 1)^4}{(4x^3 - 4x)^2} \pmod{p} \quad \text{for some } x \in \mathbb{Z} \\ &\iff n \equiv \frac{(x^2 + 1)^2}{4x^3 - 4x} \pmod{p} \quad \text{for some } x \in \mathbb{Z}. \end{aligned}$$

So the theorem is proved.

REFERENCES

- [BE] B.C. Berndt and R.J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory **11** (1979), 349-398. MR **81j**:10054
- [BEW] B.C. Berndt, R.J. Evans and K.S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, Inc., New York, Chichester, 1998, p. 58. MR **99d**:11092
- [D] H. Davenport, *The Higher Arithmetic*, 5th edition, Cambridge University Press, London, New York, 1982, pp. 74-76. MR **84a**:10001
- [J] E. Jacobsthal, *Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe zweier Quadrate*, J. Reine Angew. Math. **132** (1907), 238-245.
- [S] Zhi-Hong Sun, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), 361-377. MR **2002c**:11007

DEPARTMENT OF MATHEMATICS, HUAIYIN TEACHERS COLLEGE, HUAIAN, JIANGSU 223001, PEOPLE'S REPUBLIC OF CHINA

E-mail address: `hyzhsun@public.hy.js.cn`