Proc. Amer. Math. Soc. 130(2002), no. 9, 2503-2507

CONSECUTIVE NUMBERS WITH THE SAME LEGENDRE SYMBOL

Zhi-Hong Sun

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 $\left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right)$ or $\left(\frac{n-1}{p}\right) = \left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right)$, where $\left(\frac{\cdot}{p}\right)$ 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])

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

and

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

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*

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

and

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

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*

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

We remark that if $p\equiv 1\pmod 4$ then g is a primitive root (mod 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 $n\not\equiv 0,\pm1\pmod p$. Then*

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

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 $\left(\frac{n}{p}\right)$ 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 $s\ne t$, then $g^{s+t}\not\equiv 1\pmod p$ and so $g^s-g^t\ne(g^s-g^t)/g^{s+t}\pmod p$. This implies that $g^s+g^{-s}\not\equiv g^t+g^{-t}\pmod p$ and so $g^t(g^s-1)^2\not\equiv g^s(g^t-1)^2\pmod p$. Hence $m_s\not\equiv m_t\pmod p$. Since

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

by (1) and (2), we obtain

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

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

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

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

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

where $\mathrm{tr}(\cdot)$ 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

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

From this one can check that

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

If $p \equiv 3 \pmod 4$, then $g^k + g^{-k} = g^k + g^{kp} = tr(g^k) \in F_p$. 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 $1 \leqslant s \leqslant (p-3)/8$. So 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 $g^{2(s\pm t)} \neq \pm 1$ 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) $$\sum_{n=0}^{p-1} \chi(n^2 + bn + c) = -1.$$

Set

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

and

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

Then we see that

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

and

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

So, by (3) we have

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

That is,

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

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 $\sum_{n=0}^{p}\left(\frac{n}{p}\right)=0$ 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

$$\begin{aligned}R&=\frac18\sum_{n=0}^{p-1}\big(1+\chi(n-1)\big)\big(1+\chi(n)\big)\big(1+\chi(n+1)\big)-1-\frac12\chi(2)\\&=\frac18\Big\{p+\sum_{n=0}^{p-1}\big(\chi(n^2-n)+\chi(n^2+n)+\chi(n^2-1)+\chi(n^3-n)\big)\Big\}-1-\frac12\chi(2)\\&=\frac18(p-3-2\chi(2)a)-1-\frac12\chi(2)\\&=\begin{cases}\frac{p-17}{8}-\frac{a-1}{4} & \text{if}\quad p\equiv 1\pmod 8,\\ \frac{p-5}{8}+\frac{a-1}{4} & \text{if}\quad p\equiv 5\pmod 8)\end{cases}\end{aligned}$$

and therefore

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

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

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

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, The People's Republic of China

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