ON REVERSE ORDER NUMBERS OF CERTAIN SEQUENCES AND THE JACOBI SYMBOL

Xia Jianguo

Department of Mathematics, Nanjing Normal University, Nanjing 210097, P.R. China
e-mail: jgxia@pine.njnu.edu.cn

Qin Hourong

Department of Mathematics, Nanjing University, Nanjing 210097, P.R. China
e-mail: hrqin@netra.nju.edu.cn

(Submitted June 2003 - Final Revision December 2003)

ABSTRACT

Let $r_0, r_1, \cdots, r_{a-1}$ be the least nonnegative residues of 0, b, $2b$, $\cdots$, $(a-1)b$ modulus a. In this note, we give several recurrence formulas for the number of pairs $\{i, j\}$ with $(i-j)(r_i-r_j) < 0$. These formulas together with Zolotareff's lemma give a proof of the Law of Reciprocity for Legendre symbol. Furthermore, we prove that if a is a positive odd integer and b an integer with $(a, b) = 1$, then the permutation $r_0, r_1, \cdots, r_{a-1}$ is even or odd according as the value of Jacobi symbol is 1 or -1. This gives an arithmetic meaning of Jacobi symbol.

1. INTRODUCTION

For any sequence of real numbers

$$\alpha_1, \alpha_2, \cdots, \alpha_m,$$

the number

$$\sum_{i=2}^{m} \#\{j : j < i, \alpha_j > \alpha_i\}$$

is called *the reverse order number* of the sequence $\alpha_1, \cdots, \alpha_m$. Let a be a positive integer, b an integer and

$$r_i \equiv bi \pmod{a}, \quad 0 \le r_i < a - 1.$$

We use $P(a, b)$ to denote the sequence $r_0, r_1, \cdots, r_{a-1}$ and $\tau(a, b)$ to denote the reverse order number of $P(a, b)$.

In 1872, Zolotareff [4] proved that (see also Riesz [2] or Slavutskii [3])

Zolotareff's Lemma: *Let p be an odd prime not dividing b. Then*

$$\left(\frac{b}{p}\right) = (-1)^{\tau(p,b)}.$$

We may ask the following question:

What is the explicit formula for $\tau(p, b)$ if p is an odd prime?

In this note we give several recurrence formulas for $\tau(a, b)$, which together with Zolotareff's lemma give a proof of the Law of Reciprocity for the Legendre symbol. Furthermore, we prove that if a is a positive odd integer and $(a, b) = 1$, then $\tau(a, b)$ is even or odd according to whether the value of Jacobi symbol is 1 or -1, where the notation (a,b) denotes the greatest common divisor of a and b. This gives an arithmetic meaning of Jacobi symbol.

In this note, the following results are proved.

Theorem 1: *Let a be a positive integer and b an integer. Then*

$$\tau(a,b)=(a,b)\tau\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)+\frac{1}{4}a\left((a,b)-1\right)\left(\frac{a}{(a,b)}-1\right).$$

The proof of Theorem 1 is easy. We omit the proof.

It is clear that $\tau(a,b_1)=\tau(a,b_2)$ if $b_1\equiv b_2 \pmod a$, and $\tau(a,0)=0$, $\tau(a,1)=0$, $\tau(1,b)=0$. Thus we need only to consider $a>b>1$ and $(a,b)=1$.

Theorem 2: *Let a,b,q,r be positive integers with $(a,b)=1$ and $a=bq+r$, $1\le r<b$. Then*

$$\tau(a,b)=\frac{1}{4}b(b-1)q(q+1)+(q+1)\tau(r,b)-q\tau(b-r,r).$$

Corollary 1: *Let $a>b>1$ with $(a,b)=1$. Then*

$$\tau(a,b)=\tau(a-b,b)-\tau(b,a)+\frac{1}{2}(a-1)(b-1).$$

Corollary 2: *Let a,b,q and r be as in Theorem 2. Then*

$$\tau(a,b)=\tau(r,b)-q\tau(b,a)+\frac{1}{2}(a-1)(b-1)q-\frac{1}{4}b(b-1)q(q-1).$$

Remark: For any given b we can give an explicit formula for $\tau(a,b)$. For example, $\tau(a,2)=(a^2-1)/8$ if a is an odd number.

Theorem 3: *Let a,b be positive odd integers with $(a,b)=1$. Then*

$$\tau(a,b)+\tau(b,a)\equiv\frac{1}{4}(a-1)(b-1)\pmod 2.$$

Remark: Theorem 3 and Zolotareff's lemma give a proof of the Law of Reciprocity for the Legendre symbol. Theorem 3 is significant because we can use it together with the identity $\tau(a,b)+\tau(a,a-b)=(a-1)(a-2)/2$ to calculate the Legendre symbol without using the Jacobi symbol.

Theorem 4: *Let a be a positive odd integer and b an integer with $(a,b)=1$. Then*

$$\left(\frac{b}{a}\right)=(-1)^{\tau(a,b)},$$

where $\left(\frac{b}{a}\right)$ is the value of Jacobi symbol.

2. PROOFS

In this section, let a,b,q,r be as in Theorem 2. For $0\le i<r$, let m_i be the integer such that

$$0\le bi-m_ir<r.$$

For $1 \le i \le b-r$, let n_i be the integer such that

$$0 \le -ir + (b-r)n_i < b-r.$$

Then $0 \le m_i < b$ and $1 \le n_i \le r$. Thus we have

$$\begin{aligned} bi - m_i r &= bi - m_i(a-bq) \\ &= b(m_i q + i) - m_i a = r_{m_i q + i}, \end{aligned} \tag{1}$$

and

$$\begin{aligned} -ir + (b-r)n_i &= bn_i - r(n_i + i - 1) - r \\ &= bn_i - (a-bq)(n_i+i-1) - r \\ &= b(n_i + q(n_i+i-1)) - (n_i+i-1)a - r \\ &= r_{n_i+q(n_i+i-1)} - r. \end{aligned} \tag{2}$$

Let

$$u_i = m_i q + i \quad (0 \le i < r)$$

and

$$v_i = n_i + q(n_i + i - 1) \quad (1 \le i \le b-r).$$

Lemma 1:

$$u_{i+1} > u_i \quad (0 \le i < r-1), \qquad 0 \le u_i < a \quad (0 \le i < r);$$

$$v_{i+1} > v_i \quad (1 \le i < b-r), \qquad 1 \le v_i < a \quad (0 \le i \le b-r).$$

Proof: Since $m_{i+1} > m_i$, $n_{i+1} \ge n_i$, $q > 0$, $0 \le m_i < b$ and $1 \le n_i \le r$, Lemma 1 is proved.

Since $r_{u_i} < r \le r_{v_j}$, we have $u_i \ne v_j$ for $0 \le i < r$ and $1 \le j \le b-r$. Rearrange $u_0, u_1, \cdots, u_{r-1}, v_1, \cdots, v_{b-r}$ in increasing order as $l_0, l_1, \cdots, l_{b-1}$. Then $r_{l_i} < r$ is equivalent to that l_i is one of $u_0, u_1, \cdots, u_{r-1}$.

Lemma 2:

$$P(r,b) = \{r_{u_0}, r_{u_1}, \cdots, r_{u_{r-1}}\},$$

$$P(b-r,-r) = \{r_{v_{b-r}} - r, r_{v_1} - r, r_{v_2} - r, \cdots, r_{v_{b-r-1}} - r\}$$

and

$$P(b,-a) = \{r_{l_0}, r_{l_1}, \cdots, r_{l_{b-1}}\}.$$

Proof: The conclusions for $P(r,b)$ and $P(b-r,-r)$ follow from (1), (2) and the definitions of u_i and v_j. Now we prove the conclusion for $P(b,-a)$. By (1) and (2) we have that each r_{l_i} has the form $bl_i - p_i a$ $(0 \le i \le b-1)$. Since

$$0 \le r_{l_i} < b \text{ and } 0 \le l_0 < l_1 < \cdots < l_{b-1} < a,$$

we have $0 \le p_0 < p_1 < \cdots < p_{b-1} < b$, whence $p_i = i (0 \le i \le b-1)$. This completes the proof of Lemma 2.

Lemma 3: *Let $l_b = a$. Then for $i = 0, 1, 2, \cdots, b-1$,*

$$l_{i+1} - l_i = \begin{cases} q, & \text{if } r_{l_i} \geq r, \\ q+1, & \text{if } r_{l_i} < r, \end{cases}$$
$$r_{l_i+k} = r_{l_i} + kb, \quad \text{if } 0 \leq k < l_{i+1} - l_i.$$

Proof: Since there are exactly b numbers in $P(a,b)$ which are less than b, these b numbers are $r_{l_0}, r_{l_1}, \cdots, r_{l_{b-1}}$. If $r_{l_i} \geq r(i < b-1)$, then

$$r_{l_i} + (q-1)b < b + (q-1)b < a,$$

$$0 \leq r_{l_i} + qb - a < b + qb - a < b.$$

So $l_{i+1} - l_i = q(i < b-1)$ and $r_{l_i+k} = r_{l_i} + kb$ if $0 \leq k < q$. If $r_{l_i} < r(i < b-1)$, similarly, we have $l_{i+1} - l_i = q+1$ and $r_{l_i+k} = r_{l_i} + kb$ if $0 \leq k < q+1$. Since l_{b-1} is determined by $0 \leq bl_{b-1} - (b-1)a < b$, we have $l_{b-1} = a - q$ and $r_{l_{b-1}} = bl_{b-1} - (b-1)a = r$. Thus, $l_b - l_{b-1} = q$ and $r_{l_{b-1}+k} = r_{l_{b-1}} + kb$ if $0 \leq k < q$. This completes the proof of Lemma 3.

Let

$$\sigma_i = \#\{j : j < i, r_j > r_i\},$$

$$\delta_{u_i} = \#\{j : j < i, r_{u_j} > r_{u_i}\}$$

and

$$\tau_{v_i} = \#\{j : j < i, r_{v_j} < r_{v_i}\}.$$

Lemma 4:

$$\sum_{k=0}^{l_{j+1}-l_j-1} \sigma_{l_j+k} = \begin{cases} \frac{1}{2}q(q+1)j + (q+1)\delta_{l_j}, & \text{if } r_{l_j} < r, \\ \frac{1}{2}q(q+1)j - q\tau_{l_j}, & \text{if } r_{l_j} \geq r, \end{cases} \quad j = 0, 1, \cdots, b-1.$$

Proof: For $0 \leq i < j$ and $0 \leq k < l_{j+1} - l_j$ we consider

$$r_{l_i}, r_{l_i+1}, \cdots, r_{l_i+k}, \cdots, r_{l_{i+1}-1}. \tag{$I_i(k)$}$$

(Note. If $k = q$ and $r_{l_i} \geq r$, the term r_{l_i+k} does not appear in $(I_i(k))$). Noting that $0 \leq r_{l_i} < b$ and $0 \leq r_{l_j} < b$, by Lemma 3 we have

$$r_{l_i+t} < r_{l_j+k}, \qquad \text{if } 0 \leq t < k < l_{j+1} - l_j;$$

$$r_{l_i+t} > r_{l_j+k}, \qquad \text{if } 0 \leq k < t < l_{i+1} - l_i,$$

and $r_{l_i+k} < r_{l_j+k}$ is equivalent to $r_{l_i} < r_{l_j}$ if $0 \leq k < \min\{l_{i+1} - l_i, l_{j+1} - l_j\}$.

First, we assume that $r_{l_j} < r$. If $r_{l_i} \geq r$ or $r_{l_i} < r_{l_j}$, then by Lemma 3 there are $q-k$ numbers in $(I_i(k))$ which exceed r_{l_j+k}. If $r_{l_j} < r_{l_i} < r$, then by Lemma 3 there are $q+1-k$ numbers in $(I_i(k))$ which exceed r_{l_j+k}. Thus we have

$$\sigma_{l_j+k} = (q-k)j + \delta_{l_j}. \tag{3}$$

Now we assume that $r_{l_j} \geq r$. If $r_{l_i} < r$ or $r_{l_i} > r_{l_j}$, then by Lemma 3 there are $q-k$ numbers in $(I_i(k))$ which exceed r_{l_j+k}. If $r_{l_j} > r_{l_i} \geq r$, then by Lemma 3 there are $q-k-1$ numbers in $(I_i(k))$ which exceed r_{l_j+k}. Thus we have

$$\delta_{l_j+k} = (q-k)j - \tau_{l_j}, \tag{4}$$

and Lemma 4 follows from (3), (4) and Lemma 3.

Proof of Theorem 2: By Lemma 4 we have

$$\begin{aligned}\tau(a,b) &= \sum_{j=0}^{b-1} \sum_{k=0}^{l_{j+1}-l_j-1} \sigma_{l_j+k} \\ &= \frac{1}{4}q(q+1)b(b-1) + (q+1)\sum_{i=0}^{r-1}\delta_{u_i} - q\sum_{j=1}^{b-r}\tau_{v_j}.\end{aligned}$$

By Lemma 2 we have

$$\sum_{i=0}^{r-1}\delta_{u_i} = \tau(r,b).$$

Putting $r_{v_{b-r}} = r$, one gets from (2) that

$$P(b-r,r) = \{0, b-r_{v_1}, b-r_{v_2}, \cdots, b-r_{v_{b-r-1}}\}.$$

So

$$\begin{aligned}\sum_{i=1}^{b-r}\tau_{v_i} &= \sum_{i=1}^{b-r}\#\{j \,:\, j<i, r_{v_j} < r_{v_i}\} \\ &= \sum_{i=1}^{b-r}\#\{j \,:\, j<i, b-r_{v_j} > b-r_{v_i}\} = \tau(b-r,r).\end{aligned}$$

Hence

$$\tau(a,b) = \frac{1}{4}q(q+1)b(b-1) + (q+1)\tau(r,b) - q\tau(b-r,r).$$

This completes the proof of Theorem 2.

Proof of Corollary 1: By Theorem 2 we have

$$\tau(2a+b,a+b) = \frac{1}{2}(a+b)(a+b-1) - \tau(b,a) + 2\tau(a,b), \tag{5}$$

$$\tau(2a+b,a)=\frac{3}{2}a(a-1)-2\tau(a-b,b)+3\tau(b,a). \tag{6}$$

Again,

$$\tau(2a+b,a+b)+\tau(2a+b,a)=\tau(2a+b,-a)+\tau(2a+b,a)$$
$$=\frac{1}{2}(2a+b-1)(2a+b-2). \tag{7}$$

By (5), (6) and (7) we obtain a proof of Corollary 1.

Proof of Corollary 2: By Corollary 1, for $i=0,1,\cdots,q-1$, we have

$$\tau(a-ib,b)=\tau(a-(i+1)b,b)-\tau(b,a-ib)+\frac{1}{2}(b-1)(a-ib-1)$$
$$=\tau(a-(i+1)b,b)-\tau(b,a)+\frac{1}{2}(b-1)(a-ib-1).$$

Adding up these equalities, we obtain a proof of Corollary 2.

Proof of Theorem 3: Since $\tau(a,1)=\tau(1,a)=0$, we have

$$\tau(a,1)+\tau(1,a)=\frac{1}{4}(a-1)(1-1) \pmod 2.$$

So Theorem 3 is true for $a+b\le 4$. We use induction on $a+b$. Suppose that Theorem 3 is true for $a+b\le 2n$. Assume that a,b are positive odd integers with $a+b=2n+2$, $a>b>1$ and $(a,b)=1$. Let $a=bq+r$ with $0\le r\le b-1$. By $(a,b)=1$ and $a>b>1$ we have $r>0$. Thus, by virtue of Theorem 2 we have

$$\tau(a,b)=\frac{1}{4}b(b-1)q(q+1)+(q+1)\tau(r,b)-q\tau(b-r,r). \tag{8}$$

Since $(b,r)=1$, we have

$$\tau(b,b-r)+\tau(b,r)=\tau(b,-r)+\tau(b,r)=\frac{1}{2}(b-1)(b-2). \tag{9}$$

Hence

$$\tau(b,a)=\tau(b,r)=(q+1)\tau(b,r)+q\tau(b,b-r)-\frac{1}{2}q(b-1)(b-2). \tag{10}$$

If r is odd, then q is even. By (8), (10), $bq=a-r$ and the inductive hypothesis we have

$$\tau(a,b)+\tau(b,a)\equiv\frac{1}{4}(b-1)(a-r)(q+1)+\tau(r,b)+\tau(b,r)$$
$$\equiv\frac{1}{4}(b-1)(a-r)+\tau(r,b)+\tau(b,r)$$
$$\equiv\frac{1}{4}(b-1)(a-r)+\frac{1}{4}(b-1)(r-1)\equiv\frac{1}{4}(a-1)(b-1) \pmod 2.$$

If r is even, then both $b-r$ and q are odd. By (8), (10), $b(q+1)=a+b-r$ and the inductive hypothesis we have

$$\begin{aligned}\tau(a,b)+\tau(b,a) &\equiv \frac{1}{4}(b-1)(a+b-r)q+\tau(b-r,r)+\tau(b,b-r)+\frac{1}{2}q(b-1)b\\ &\equiv \frac{1}{4}(b-1)(a+b-r)+\tau(b-r,b)+\tau(b,b-r)+\frac{1}{2}(b-1)b\\ &\equiv \frac{1}{4}(b-1)(a+b-r)+\frac{1}{4}(b-r-1)(b-1)+\frac{1}{2}(b-1)b\\ &\equiv \frac{1}{4}(a-1)(b-1) \pmod 2.\end{aligned}$$

This completes the proof of Theorem 3.

Proof of Theorem 4: We use induction on a. First, it is easy to see that Theorem 4 is true for $b=1$. Second, If $b_1 \equiv b_2 \pmod a$, then

$$\left(\frac{b_1}{a}\right)=\left(\frac{b_2}{a}\right), \quad \tau(a,b_1)=\tau(a,b_2).$$

Thus, without loss of generality, we may assume that $a>b>1$. Since

$$\tau(3,2)=1, \quad \left(\frac{2}{3}\right)=-1,$$

Theorem 4 is true for $a=3$. Suppose that Theorem 4 is true for $a\le 2n-1$ $(n\ge 2)$. Now, let $a=2n+1$. If b is a positive odd integer with $(a,b)=1$ and $a>b>1$, then, by the Law of Reciprocity for the Jacobi symbol, the inductive hypothesis and Theorem 3, we have

$$\left(\frac{b}{a}\right)=\left(\frac{a}{b}\right)(-1)^{\frac{1}{4}(a-1)(b-1)}=(-1)^{\tau(b,a)}(-1)^{\frac{1}{4}(a-1)(b-1)}=(-1)^{\tau(a,b)}.$$

If b is a positive even integer with $(a,b)=1$ and $a>b>1$, then $a-b$ is odd and by (9),

$$\begin{aligned}\left(\frac{b}{a}\right) &= \left(\frac{a-b}{a}\right)\left(\frac{-1}{a}\right)\\ &= (-1)^{\tau(a,a-b)}(-1)^{\frac{1}{2}(a-1)}\\ &= (-1)^{\tau(a,-b)}(-1)^{\frac{1}{2}(a-2)(a-1)}\\ &= (-1)^{\tau(a,b)}.\end{aligned}$$

This completes the proof.

ACKNOWLEDGMENTS

We would like to thank Professor Chen Yonggao for his help in preparing this paper. The research is supported by the NSFC, SRFDP and the 973 Grant.

REFERENCES

[1] J. H. Conway. "The Sensual (quadratic) Form." Carus Mathematical Monographs 26, Mathematical Association of America, Washington DC, 1997.
[2] M. Riesz. "Sur le lemme de Zolotareff et sur la loi de réciprocité des restes quadratiques." *Math. Scand.* **1** (1953): 159-169.
[3] I. S. Slavutskii. "A Generalization of a Lemma of Zolotarev." (Russian) *Rev. Math. Pures Appl.* (Bucarest) **8** (1963): 455-457.
[4] E. I. Zolotareff. "Nouvelle démonstration de la loi de réciprocité de Legendre." *Nouv. Ann. Math.*, Rap. **11.2** 1955-013 (1872): 354-362.

AMS Classification Numbers: 11A07

✠ ✠ ✠