IJMMS 31:11 (2002) 701–702
PII. S0161171202202197
http://ijmms.hindawi.com


# A NOTE ON A PAPER BY BRENNER

PAVLOS TZERMIAS

Received 4 February 2002

We note that a result of Brenner (1962) follows from a theorem of Lerch (1896) which also extends it.

2000 Mathematics Subject Classification: 11A15, 05A05.

Let $m$ and $n$ be relatively prime integers with $n \geq 2$. Let $\sim$ be the equivalence relation on the set $S = (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ given by $t_1 \sim t_2$ if and only if there exists an integer $k$ such that $m^k t_1 = t_2$. Denote by $N$ the number of equivalence classes. Brenner proved the following result [1].

**Theorem 1.** *If $n$ is odd, then $(-1)^N$ equals the Jacobi symbol $(m/n)$.*

The purpose of this note is to point out that the above result is a consequence of a theorem of Lerch [3] dating back to 1896, which, moreover, extends Theorem 1 to the case of even $n$.

**Theorem 2** (Lerch). *For relatively prime integers $m$ and $n$, with $n \geq 2$, the sign of the permutation $\pi$ induced by multiplication by $m$ on $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ equals*
(a) *the Jacobi symbol $(m/n)$ if $n$ is odd;*
(b) *$1$ if $n$ is even and not divisible by $4$;*
(c) *$(-1)^{(m-1)/2}$ if $n$ is divisible by $4$.*

Observe that $N$ is the number of cycles $\tau_1, \dots, \tau_N$ in the decomposition of $\pi$ into a product of disjoint cycles (1-cycles need to be included). Now if $l_i$ is the length of $\tau_i$, then the sign of $\tau_i$ equals $(-1)^{l_i - 1}$, so, if $n$ is odd, the sign of $\pi$ equals

$$(-1)^{\sum_{i=1}^{N}(l_i-1)} = (-1)^{n-1-N} = (-1)^N. \tag{1}$$

Thus Theorem 1 follows from Theorem 2, as does the following extension.

**Corollary 3.** *For $n$ even $(-1)^N$ equals $-1$, if $n \equiv 2 (\mathrm{mod}\, 4)$, and $(-1)^{(m+1)/2}$, if $n \equiv 0 (\mathrm{mod}\, 4)$.*

Lerch's theorem, which generalizes a result of Zolotareff [4] on the Legendre symbol, considerably simplifies the theory of quadratic residues (see, e.g., [2]) and deserves to be more widely known.

## References

[1] J. L. Brenner, *A new property of the Jacobi symbol*, Duke Math. J. **29** (1962), 29–31.
[2] F. Hirzebruch and D. Zagier, *The Atiyah-Singer Theorem and Elementary Number Theory*, Mathematics Lecture Series, no. 3, Publish or Perish, Massachusetts, 1974.

[3] M. Lerch, *Sur un théorème de Zolotarev*, Bull. Intern. de l'Acad. François Joseph **3** (1896), 34–37 (French).

[4] G. Zolotareff, *Nouvelle demonstration de la loi de réciprocité de Legendre*, Nouvelles Annales de Math. **11** (1872), no. 2, 354–362 (French).

Pavlos Tzermias: Department of Mathematics, University of Tennessee, Knoxville, TN 37996, USA

*E-mail address*: tzermias@math.utk.edu