ACTA ARITHMETICA
170.1 (2015)

Equality of Dedekind sums modulo $8\mathbb{Z}$

by

EMMANUEL TSUKERMAN (Berkeley, CA)

1. Background. Dedekind sums are classical objects of study introduced by Richard Dedekind in the 19th century in his study of the η-function [Ded53]. Among many other areas of mathematics, Dedekind sums appear in: geometry (lattice point enumeration in polytopes [BR07]), topology (signature defects of manifolds [HZ74]) and algorithmic complexity (pseudorandom number generators [Knu98]). To define the Dedekind sums, let

$$((x)) = \begin{cases} x - \lfloor x \rfloor - 1/2 & \text{if } x \in \mathbb{R} \setminus \mathbb{Z}, \\ 0 & \text{if } x \in \mathbb{Z}. \end{cases}$$

Then the *Dedekind sum* $s(a,b)$ for $a, b \in \mathbb{N}$ coprime is defined by

$$s(a,b) = \sum_{k=1}^{b} \left(\left(\frac{ak}{b}\right)\right)\left(\left(\frac{k}{b}\right)\right).$$

Recently, Jabuka et al. [JRW11] raise the question of when two Dedekind sums $s(a_1, b)$ and $s(a_2, b)$ are equal. In the same paper, they prove the necessary condition $b \mid (a_1a_2 - 1)(a_1 - a_2)$. Girstmair [Gir14] shows that this condition is equivalent to $12s(a_1, b) - 12s(a_2, b) \in \mathbb{Z}$. In [Tsu14], necessary and sufficient conditions for $12s(a_1, b) - 12s(a_2, b) \in 2\mathbb{Z}, 4\mathbb{Z}$ are given.

In this note we give necessary and sufficient conditions for $12s(a_1, b) - 12s(a_2, b) \in 8\mathbb{Z}$ by using a generalization of Zolotarev's classical lemma relating the Jacobi symbol to the sign of a special permutation ([1]) due to Lerch [Ler96]. Along the way, we resolve a conjecture of Girstmair [Gir15] about the alternating sum of partial quotients modulo 4.

2010 *Mathematics Subject Classification*: Primary 11F20.
Key words and phrases: Dedekind sums, Zolotarev's lemma, Barkan–Hickerson–Knuth formula.

([1]) The motivation behind Zolotarev's work was to produce a proof of the law of quadratic reciprocity.

2. Preliminaries. Let $\pi_{(a,b)} \in \mathrm{Aut}(\mathbb{Z}/b\mathbb{Z})$, $\pi_{(a,b)} : x \mapsto ax$. Let $[x]_b = x - b\lfloor x/b \rfloor$ be the function taking $x \in \mathbb{Z}/b\mathbb{Z}$ to its smallest nonnegative representative. We view $\pi_{(a,b)}$ as a permutation of $\{0, 1, \dots, b-1\}$ given by

$$\pi_{(a,b)} = \begin{pmatrix} 0 & 1 & \cdots & b-1 \\ [\pi(0)] & [\pi(1)] & \cdots & [\pi(b-1)] \end{pmatrix} = \begin{pmatrix} 0 & 1 & \cdots & b-1 \\ 0 & [a]_b & \cdots & [(b-1)a]_b \end{pmatrix}.$$

The precedent for doing so is already present in the work of Zolotarev, in which he relates the sign of $\pi_{(a,b)}$ to the Jacobi symbol $\left(\frac{a}{b}\right)$ and obtains a proof of the law of quadratic reciprocity (see, e.g., [RG72, p. 38]). Let $I(a,b)$ denote the number of inversions of $\pi_{(a,b)}$.

THEOREM 2.1 (Zolotarev). *For odd b and $(a,b) = 1$,*

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

The following result shows that the inversions of $\pi_{(a,b)}$ and Dedekind sums are closely related.

THEOREM 2.2 (Meyer, [Mey57]). *The number of inversions $I(a,b)$ of $\pi_{(a,b)}$ is equal to*

$$I(a,b) = -3bs(a,b) + \tfrac{1}{4}(b-1)(b-2),$$

where $s(a,b)$ is the Dedekind sum.

From the reciprocity law of Dedekind sums, one obtains a reciprocity law for inversions.

THEOREM 2.3 (Salié, [Mey57, p. 163]). *For all coprime $a, b \in \mathbb{N}$,*

$$4aI(a,b) + 4bI(b,a) = (a-1)(b-1)(a+b-1). \tag{2.1}$$

Let a and b be positive integers, $a < b$. Consider the regular continued fraction expansion

$$\frac{a}{b} = [0, a_1, \dots, a_n],$$

where all digits $a_1, \dots, a_n$ are positive integers. We assume that n is odd ([2]). We will be interested in

$$T(a,b) = \sum_{j=1}^{n} (-1)^{j-1} a_j \quad \text{and} \quad D(a,b) = \sum_{j=1}^{n} a_j.$$

With this notation, we have:

([2]) If n is even, we can consider $[0, a_1, \dots, a_{n-1}, a_n - 1, 1]$ instead.

THEOREM 2.4 (Barkan–Hickerson–Knuth formula). *Let $a, b \in \mathbb{N}$ be coprime and let $a^*a \equiv 1 \pmod{b}$ with $0 < a^* < b$. Then*

$$12s(a,b) = T(a,b) + \frac{a+a^*}{b} - 3.$$

In [Ler96], Lerch improves upon Zolotarev's lemma by determining the parity of $I(a,b)$ when b is even:

THEOREM 2.5 (Lerch).

$$I(a,b) \equiv \begin{cases} \left(1 - \left(\frac{a}{b}\right)\right)/2 \pmod{2} & \text{if } b \text{ is odd,} \\ (a-1)(b+a-1)/4 \pmod{2} & \text{if } b \text{ is even.} \end{cases}$$

Proof. We assume that b is even, as the result for b odd follows from Theorem 2.1. Reducing equality (2.1) modulo 8 and using the assumption that b is even yields

$$4aI(a,b) \equiv (a-1)(b-1)(a+b-1) \pmod{8}.$$

Since $a-1$ and $a+b-1$ are even,

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

from which the claim follows. ∎

For further generalizations of Zolotarev's lemma, see [BC14].

3. Main results. As a consequence of Theorem 2.5, we are able to show the following necessary and sufficient conditions for equality of Dedekind sums modulo $8\mathbb{Z}$.

THEOREM 3.1. *Let $a_1, a_2 \in \mathbb{N}$ be relatively prime to $b \in \mathbb{N}$. The following are equivalent:*

(a) $I(a_1,b) \equiv I(a_2,b) \pmod{2b}$.
(b) $3s(a_1,b) - 3s(a_2,b) \in 2\mathbb{Z}$.
(c) *Define*

$$\mu(a,b) = \begin{cases} \left(1 - \left(\frac{a}{b}\right)\right)/2 & \text{if } b \text{ is odd,} \\ (a-1)(b+a-1)/4 & \text{if } b \text{ is even.} \end{cases}$$

Then

$$(a_1-a_2)(b-1)(b+a_1a_2-1) \equiv 4b(a_2\mu(b,a_1) - a_1\mu(b,a_2)) \pmod{8b}.$$

We also determine $T(a,b)$ modulo 8:

THEOREM 3.2. *Let $a, b \in \mathbb{N}$ be coprime. Then*

$$bT(a,b) \equiv -4\mu(a,b) + b^2 + 2 - a - a^* \pmod{8}. \tag{3.1}$$

Reducing further modulo 4 and modulo 2 resolves a conjecture of Girstmair [Gir15].

4. Proofs and examples

Proof of Theorem 3.1. The equivalence of (a) and (b) follows from Theorem 2.2. Reducing equation (2.1) of Theorem 2.3 modulo $8b$ and using Theorem 2.5 yields

$$4aI(a,b) + 4b\mu(b,a) \equiv (a-1)(b-1)(a+b-1) \pmod{8b}. \ \blacksquare$$

That Theorem 3.1 is not a sufficient condition for the equality of two Dedekind sums is demonstrated in the following example.

EXAMPLE 4.1. Take $a_1 = 1$, $a_2 = 15$ and $b = 49$. Then

$$\left(\frac{b}{a_1}\right) = 1, \quad \left(\frac{b}{a_2}\right) = 1.$$

We have

$$(a_1 - a_2)(b-1)(b + a_1 a_2 - 1) = -42336 = 108 \cdot 8 \cdot 49 \equiv 0 \pmod{8b}.$$

Thus we expect $3s(a_1,b) - 3s(a_2,b) \in 2\mathbb{Z}$. Indeed,

$$s(a_1,b) = \frac{188}{49}, \qquad s(a_2,b) = -\frac{8}{49},$$

so that

$$3s(a_1,b) - 3s(a_2,b) = 12.$$

Equality does not hold.

Proof of Theorem 3.2. By Theorems 2.2 and 2.4, we have

$$bT(a,b) = 12bs(a,b) - a - a^* + 3b = -4I(a,b) + b^2 + 2 - a - a^*.$$

Reducing modulo 8 and using Theorem 2.5 leads to

$$bT(a,b) \equiv -4\mu(a,b) + b^2 + 2 - a - a^* \pmod 8. \ \blacksquare$$

Let $k \in \mathbb{Z}$ satisfy $aa^* = 1 + kb$. In [Gir15], Girstmair conjectures that if $a \equiv a^* \equiv 0 \pmod 2$, then:

(i) If a or a^* is $\equiv 2 \pmod 4$, then $T(a,b) \equiv (b-k)/2 \pmod 4$.
(ii) If a and a^* are both $\equiv 0 \pmod 4$, then $T(a,b) \equiv (k-b)/2 \pmod 4$.
(iii) If a and a^* are both $\equiv 0 \pmod 4$, then $D(a,b)$ is odd.

We now show how this follows from Theorem 3.2. Reducing congruence (3.1) modulo 4 gives

$$bT(a,b) \equiv b^2 + 2 - a - a^* \pmod 4.$$

Assume first that $a \equiv a^* \equiv 0 \pmod 4$. Then

$$bT(a,b) \equiv b^2 + 2 \equiv -1 \pmod 4 \ \Rightarrow \ T(a,b) \equiv -b^{-1} \equiv -b \pmod 4.$$

On the other hand,

$$1 + kb \equiv 0 \pmod 8 \ \Rightarrow \ k \equiv -b \pmod 8.$$

This proves (ii). As Girstmair notes, part (iii) follows from (ii).

Next we show (i). It suffices to prove the result when $a \equiv 2 \pmod 4$, since $T(a,b) = T(a^*,b)$. We have

$$bT(a,b) \equiv 1 - a^* \pmod 4 \;\Rightarrow\; T(a,b) \equiv b^{-1}(1-a^*) \equiv b(1-a^*) \pmod 4.$$

On the other hand,

$$\frac{b-k}{2} \equiv \frac{b - b^{-1}(aa^*-1)}{2} \equiv b - \frac{baa^*}{2} \equiv b - ba\left(\frac{a^*}{2}\right) \equiv b - ba^* \pmod 4,$$

completing the proof.

This, together with the results in [Gir15], determines $T(a,b)$ and $D(a,b)$ in all cases.

Acknowledgements. The author would like to thank Kurt Girstmair and Pete Clark for helpful comments and bibliographic references.

This material is based upon work supported by the National Science Foundation Graduate Research Fellowship under Grant No. DGE 1106400. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors(s) and do not necessarily reflect the views of the National Science Foundation.

References

[BR07] M. Beck and S. Robins, *Computing the Continuous Discretely. Integer-Point Enumeration in Polyhedra*, Undergrad. Texts Math., Springer, New York, 2007.

[BC14] A. Brunyate and P. L. Clark, *Extending the Zolotarev–Frobenius approach to quadratic reciprocity*, Ramanujan J. 37 (2015), 25–50.

[Ded53] R. Dedekind, *Erläuterungen zu den Fragmenten xxviii*, in: Collected Works of Bernhard Riemann, Dover, New York, 1953, 466–478.

[Gir14] K. Girstmair, *A criterion for the equality of Dedekind sums mod* $\mathbb{Z}$, Int. J. Number Theory 10 (2014), 565–568.

[Gir15] K. Girstmair, *Congruences modulo 4 for the alternating sum of the partial quotients*, arXiv:1501.00655 (2015).

[HZ74] F. Hirzebruch and D. Zagier, *The Atiyah–Singer Theorem and Elementary Number Theory*, Math. Lecture Ser. 3, Publish or Perish, Boston, MA, 1974.

[JRW11] S. Jabuka, S. Robins, and X. Wang, *When are two Dedekind sums equal?*, Int. J. Number Theory 7 (2011), 2197–2202.

[Knu98] D. E. Knuth, *The Art of Computer Programming. Vol. 2. Seminumerical Algorithms*, Addison-Wesley, Boston, MA, 3rd ed., 1998.

[Ler96] M. Lerch, *Sur un théorème de Zolotarev*, Bull. Int. Acad. François Joseph 3 (1896), 34–37.

[Mey57] C. Meyer, *Über einige Anwendungen Dedekindscher Summen*, J. Reine Angew. Math. 198 (1957), 143–203.

[RG72] H. Rademacher and E. Grosswald, *Dedekind Sums*, Carus Math. Monogr. 16, Math. Assoc. America, Washington, DC, 1972.

[Tsu14] E. Tsukerman, *Equality of Dedekind sums mod* $\mathbb{Z}$, $2\mathbb{Z}$ *and* $4\mathbb{Z}$, Int. J. Number Theory (2014) (online).

Emmanuel Tsukerman
Department of Mathematics
University of California
Berkeley, CA 94720-3840, U.S.A.
E-mail: e.tsukerman@berkeley.edu

Received on 21.1.2015
and in revised form on 7.5.2015 (8060)