JOURNAL OF NUMBER THEORY 19, 1–6 (1984)

Arithmetic Properties of Heilbronn Sums

W. L. FOUCHÉ

Department of Mathematics, University of the Orange Free State, Bloemfontein, South Africa

Communicated by H. Zassenhaus

Received December 2, 1981; revised February 2, 1982

For each odd prime q an integer NH_q ($NH_3 = -1$, $NH_5 = -1$, $NH_7 = 97$, $NH_{11} = -243$,...) is defined as the norm from L to $\mathbb{Q}$ of the *Heilbronn sum* $H_q = \mathrm{Tr}_L^{\mathbb{Q}(\zeta)}(\zeta)$, where ζ is a primitive q^2th root of unity and $L \subseteq \mathbb{Q}(\zeta)$ the subfield of degree q. Various properties are proved relating the congruence properties of H_q and NH_q modulo p ($p \neq q$ prime) to the Fermat quotient $(p^{q-1} - 1)/q \pmod q$; in particular, it is shown that NH_q is even iff $2^{q-1} \equiv 1 \pmod{q^2}$.

1. INTRODUCTION

Let q be an odd prime and let ζ be a primitive q^2th root of unity. We shall study the divisibility properties of the exponential sums defined by the formula

$$H_q = \sum_{1 \leqslant \alpha \leqslant q-1} \zeta^{\alpha^q}. \tag{1.1}$$

These sums are closely related to certain n-dimensional Kloosterman sums. (See, e.g., [3, p. 342]. Smith [3] mentions that Heilbronn, approximately 15 years ago, posed the problem of finding nontrivial upper bounds for the sums $H_q + 1$. For this reason we shall call the sum in (1.1) the qth *Heilbronn sum.*

The number H_q is just $\mathrm{Tr}_L^{\mathbb{Q}(\zeta)}\zeta$, where L ($=\mathbb{Q}(H_q)$) is the subfield of $\mathbb{Q}(\zeta)$ of degree q over $\mathbb{Q}$. The rational integer $N_{\mathbb{Q}}^L(H_q)$, which we shall denote simply by NH_q, is the main object of study of this paper. A table of these numbers (and of their small prime factors) for $q < 50$ appears at the end of the paper.

For x an integer such that $(x, q) = 1$, we define the *Fermat quotient* by

$$Q(x) \equiv (x^{q-1} - 1)/q \pmod q.$$

For the history of these quotients, see [1, Chapter IV]. The importance of these quotients is derived (among other things) from their connection with

0022-314X/84 $3.00

Fermat's equation. For example, Wieferich [4] has shown that if there exist integers x, y, z which are relatively prime and not multiples of q such that $x^q + y^q + z^q = 0$ then $Q(2) \equiv 0 \pmod q$. (For more information along these lines see [2, Lectures 8, 9]. In this paper we relate the divisors of the Heilbronn sums to the solutions p of the congruence $Q(p) \equiv 0 \pmod q$. We shall prove

THEOREM 1. *Let q be an odd prime.*

(a) *If p is a prime divisor of NH_q, then $Q(p) \equiv 0 \bmod q$. If $p = 2$, q arbitrary, or if $p = 3$, $q \equiv 1 \bmod 3$, then the converse also holds.*

(b) *If p is a prime number, then*

$$Q(p) \equiv 0 \bmod q \qquad \text{if and only if } H_q^p \equiv H_q \bmod p\,O \quad \text{and} \quad q \neq p.$$

It is clear that the converse of (a) does not hold for all prime numbers p, since for fixed q there are infinitely many primes p satisfying $p^{q-1} \equiv 1 \bmod q^2$. In the course of the proof of the theorem we shall also show that for all odd primes q we have

$$NH_q \equiv -1 \bmod q^2. \tag{1.2}$$

The table in Section 3 strongly suggests that H_q is a unit only if $q = 3$ or $q = 5$. In view of (1.2) one might conjecture that $|NH_q| \geqslant q^2 - 1$ whenever $q \geqslant 7$. On the other hand, we shall see in Section 2 that $|NH_q| \leqslant (q-1)^{q/2}$ for all odd primes q.

2. HEILBRONN SUMS

Since the multiplicative group $G_q = (\mathbb{Z}/q^2\mathbb{Z})^*$ has a unique subgroup A_q of order $q-1$, it follows that $\ker \delta = A_q$ for any epimorphism $\delta\colon G_q \to \mathbb{Z}/q\mathbb{Z}$. Since $\delta(x^q) \equiv q\delta(x) \bmod q$ for any x in G_q and the set of integers $\{x^q\colon 1 \leqslant x \leqslant q-1\}$ are distinct modulo q^2, we conclude that

$$A_q = \{x^q \bmod q^2\colon 1 \leqslant x \leqslant q-1\}. \tag{2.1}$$

It is easily seen that if α, β are integers prime to q, then

$$Q(\alpha\beta) \equiv Q(\alpha) + Q(\beta) \bmod q.$$

Since $(1 + qk)^{q-1} = 1 + (q-1)\,qk + O(q^2)$, for any integer k, we have

$$Q(1 + qk) \equiv -k \bmod q.$$

Therefore, the Fermat quotient induces an epimorphism $G_q \to \mathbb{Z}/q\mathbb{Z}$ and yields a coset decomposition

$$G_q = \bigcup_{k=0}^{q-1} (1+kq) A_q. \tag{2.2}$$

Let ζ be a primitive q^2th root of unity and identify the Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ with G_q. Let L denote the fixed field with respect to the subgroup A_q. Then, by (2.1),

$$H_q = \mathrm{Tr}_L^{\mathbb{Q}(\zeta)}(\zeta).$$

Since $L/\mathbb{Q}$ is a field extension of prime degree and $H_q \notin \mathbb{Q}$, we conclude that $L = \mathbb{Q}(H_q)$. By (2.2), the conjugates of H_q can be written as

$$H_q^{(k)} = \sum_{1 \leqslant \alpha \leqslant q-1} \zeta^{\alpha k q} \zeta^{\alpha^q}$$

for $k = 0, 1, ..., q-1$. Write $\eta = \zeta^q$ and define $f(\alpha) = \zeta^{\alpha^q}$ for $\alpha \not\equiv 0 \bmod q$ and $f(\alpha) = 0$ for $\alpha \equiv 0 \bmod q$. Then $H_q^{(k)} = \sum_{\alpha \bmod q} f(\alpha)\, \eta^{k\alpha}$ by definition, so that $H_q^{(k)}$ is the "Fourier transform" of the function f on the group $(\mathbb{Z}/q\mathbb{Z})$. The Fourier inversion formula now gives

$$q\zeta^{\alpha^q} = \sum_k \eta^{-k\alpha} H_q^{(k)} \tag{2.3}$$

whenever $1 \leqslant \alpha \leqslant q-1$. In addition, since $H^{(k)}$ is real for every k we have

$$\mathrm{Tr}\, H_q^2 = q \sum_\alpha |f(\alpha)|^2 = q(q-1) \qquad \text{(Plancherel).} \tag{2.4}$$

Note that the arithmetic–geometric mean inequality when applied to $(H_q^{(k)})^2$, $0 \leqslant k \leqslant q-1$ now gives, in view of (2.4), the inequality

$$|NH_q| \leqslant (q-1)^{q/2}.$$

3. Proof of the Theorem

In the sequel we denote by O the ring of integers in $L = \mathbb{Q}(H_q)$.

Lemma 3.1. *Let q be an odd prime. Then*

(a) $NH_q \equiv -1 \bmod q$.

(b) *Let* $\mathfrak{p}$ *be a prime ideal in* O *such that* $\mathfrak{p} \cap \mathbb{Z} \neq (q)$. *Then, for some* $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ *we have* $\sigma H_q \not\equiv H_q \bmod \mathfrak{p}$.

Proof. (a) Let $\pi = \zeta - 1$. Then the principal ideal (π) is the only prime ideal in $\mathbb{Q}(\zeta)$ that lies above q. Furthermore, $\zeta^x \equiv 1 \bmod \pi$ for every x in $\mathbb{Z}$ that is prime to q. Since every Heilbronn sum σH_q is the sum of $q-1$ terms of the form ζ^x with $(x, q) = 1$, we have $\sigma H_q \equiv q - 1 \equiv -1 \bmod \pi$ for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Consequently, $NH_q \equiv (-1)^q \bmod \pi$.

(b) Suppose that $\sigma H_q \equiv H_q \bmod \mathfrak{p}$ for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Then, if $\mathfrak{P}$ is a prime in $\mathbb{Z}[\zeta]$ lying above $\mathfrak{p}$ it follows from (2.3) that

$$\zeta q \equiv H_q \sum_k \eta^{-k} \equiv 0 \bmod \mathfrak{P},$$

which is impossible if $\mathfrak{P} \neq (\pi)$.

Theorem 1(b) is a direct consequence of

LEMMA 3.2. *If* p *is a prime number, then* $p^{q-1} \equiv 1 \bmod q^2$ *if and only if* p *splits completely in* O, *which in turn is equivalent to the congruence* $H_q^p \equiv H_q \bmod p\,O$, $q \neq p$.

Proof. Let $\mathfrak{P}$ be a prime in $\mathbb{Z}[\zeta]$ that lies above p and write $\mathfrak{p} = \mathfrak{P} \cap O$. It is clear that $p^{q-1} \equiv 1 \bmod q^2$ if and only if the order of $p \bmod q^2$ is a divisor of $q-1$. This statement is equivalent to $q-1$ being divisible by the residue class degree $f(\mathfrak{P}/p)$ of $\mathfrak{P}$ with respect to p and $p \neq q$. Since $f(\mathfrak{P}|p) = f(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{p}/p)$ and $f(\mathfrak{p}/p)$ is a divisor of q, the first part of the lemma follows.

If $f(\mathfrak{p}/p) = 1$, then $O/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$ and $\alpha^q \equiv \alpha \bmod \mathfrak{p}$ for every α in O. Conversely, suppose that $H_q^p \equiv H_q \bmod \mathfrak{p}$, $p \neq q$, where $\mathfrak{p}$ is a prime ideal in O above p. We must show that $f(\mathfrak{p}/p) = 1$. If not, there exists exactly one prime $\mathfrak{p}$ above p such that $O/\mathfrak{p}$ is a field extension of $\mathbb{Z}/p\mathbb{Z}$ of degree q. The corresponding Galois group is generated by the Frobenius automorphism $x \to x^p$. If H_q satisfies the above congruence, then $H_q \bmod \mathfrak{p}$ is invariant with respect to the Galois group. Therefore, for some x in $\mathbb{Z}/p\mathbb{Z}$, we have $H_q \equiv x \bmod \mathfrak{p}$. Since $\sigma\mathfrak{p} = \mathfrak{p}$ for every σ in $\mathrm{Gal}(L/\mathbb{Q})$, we have $\sigma H_q \equiv x \bmod \mathfrak{p}$ for every σ—a contridiction in view of Lemma 3.1(b).

Proof of Theorem 1(a). Let p be a prime such that $p \mid NH_q$. Then by Lemma 3.1(a) we have $p \neq q$. Suppose that p does not split completely in O. Then, there exists a unique $\mathfrak{p}$ above p such that $\sigma H_q \equiv 0 \bmod \mathfrak{p}$ for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$—contradiction. By Lemma 3.1(b) we, therefore, have that if $p \mid NH_q$, then $p^{q-1} \equiv 1 \bmod q^2$.

Suppose now $2^{q-1} \equiv 1 \bmod q^2$ but $2 \nmid NH_q$. Since 2 splits completely in O, we have that $O/\mathfrak{p} \cong \mathbb{Z}/2\mathbb{Z}$ for every $\mathfrak{p} \mid 2$. Since $2 \nmid NH_q$, we conclude that $\sigma H_q \equiv 1 \bmod \mathfrak{p}$ for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$—a contradiction.

Suppose that $3^{q-1} \equiv 1 \bmod q^2$ but $3 \nmid NH_q$. Then, as above, $O/\mathfrak{p} \cong \mathbb{Z}/3\mathbb{Z}$ if $\mathfrak{p} \mid 3$, and, therefore, $\sigma H_q^2 \equiv 1 \bmod \mathfrak{p}$ for every σ. Consequently, by (2.4) we have

$$q(q-1) \equiv q \bmod \mathfrak{p},$$

and it follows that $q \equiv 2 \bmod 3$.

Proof of (1.2). Put $NH_q = -1 + kq$ (Lemma 3.1(a)). Then

$$(NH_q)^{q-1} \equiv 1 - kq(q-1) \equiv 1 + kq \bmod q^2.$$

But $(NH_q)^{q-1} \equiv 1 \bmod q^2$ since every prime divisor r of NH_q satisfies $r^{q-1} \equiv 1 \bmod q^2$ (Theorem 1(a)). We conclude that $k \equiv 0 \bmod q$ and the result follows.

The table below depicts the numbers NH_q for all odd primes $q \leqslant 50$ as well as their prime factors $p \leqslant 2767$.

q	NH_q	$p^v \parallel NH_q \quad (p \leqslant 2767)$
3	−1	–
5	−1	–
7	97	97
11	−243	3^5
13	12167	23^3
17	577	577
19	221874931	–
23	157112485811	–
29	−2480435158303	137
31	310695313260929	–
37	−51140551819476687829	–
41	2727257042363914863401	–
43	−2572343484535669027372727	19^4
47	1052824394331287344099620777449	53^2

Acknowledgment

The referee has kindly supplied the table. He has conjectured the congruence (1.2) and has suggested important improvements in the proofs of (2.3) and (2.4)

REFERENCES

1. L. E. DICKSON, "History of the Theory of Numbers: Vol. 1," Stechert, New York, 1934.
2. P. RIBENBOIM, "13 Lectures on Fermat's Last Theorem," Springer-Verlag, New York/Berlin, 1980.
3. R. A. SMITH, On n-dimensional Kloosterman sums, *J. Number Theory* **11** (1979), 324–343.
4. A. WIEFERICH, Zum letzten Fermat'schen Theorem, *J. Reine Angew. Math.* **136** (1909), 293–302.