MATHEMATICS OF COMPUTATION
Volume 77, Number 261, January 2008, Pages 475–493
S 0025-5718(07)02011-X
Article electronically published on May 14, 2007

EXPLICIT VALUES OF MULTI-DIMENSIONAL KLOOSTERMAN SUMS FOR PRIME POWERS, II

S. GURAK

In memory of Derick H. Lehmer

ABSTRACT. For any integer $m > 1$ fix $\zeta_m = \exp(2\pi i/m)$, and let $\mathbf{Z}_m^*$ denote the group of reduced residues modulo m. Let $q = p^\alpha$, a power of a prime p. The hyper-*Kloosterman sums of dimension* $n > 0$ are defined for q by

$$R(d,q) = \sum_{x_1,\dots,x_n \in Z_q^*} \zeta_q^{x_1+\cdots+x_n+d(x_1\cdots x_n)^{-1}} \qquad (d \in \mathbf{Z}_q^*),$$

where x^{-1} denotes the multiplicative inverse of x modulo q.

Salie evaluated $R(d,q)$ in the classical setting $n = 1$ for even q, and for odd $q = p^\alpha$ with $\alpha > 1$. Later, Smith provided formulas that simplified the computation of $R(d,q)$ in these cases for $n > 1$. Recently, Cochrane, Liu and Zheng computed upper bounds for $R(d,q)$ in the general case $n > 0$, stopping short of their explicit evaluation. Here I complete the computation they initiated to obtain explicit values for the Kloosterman sums for $\alpha > 1$, relying on basic properties of some simple specialized exponential sums. The treatment here is more elementary than the author's previous determination of these Kloosterman sums using character theory and p-adic methods. At the least, it provides an alternative, independent evaluation of the Kloosterman sums.

1. Introduction

For any integer $m > 1$ fix $\zeta_m = \exp(2\pi i/m)$ and let $\mathbf{Z}_m^*$ denote the group of reduced residues modulo m. Let $q = p^\alpha$, a power of a prime p. The hyper-Kloosterman sums of dimension $n > 0$ are defined for q by

$$R(d,q) = \sum_{x_1,\dots,x_n \in Z_q^*} \zeta_q^{x_1+\cdots+x_n+d(x_1\cdots x_n)^{-1}} \tag{1}$$

for $1 \le d \le q$, $(d,q) = 1$, where x^{-1} denotes the multiplicative inverse of x modulo q for any x in $\mathbf{Z}_q^*$. For $(a,q) = 1$, if σ_a denotes the automorphism of $\mathbf{Q}(\zeta_q)$ induced by sending $\zeta_q \to \zeta_q^a$, then it is readily seen from (1) that

$$\sigma_a(R(d,q)) = R(da^{n+1},q). \tag{2}$$

In particular, $R(d,q)$ lies in the subfield K of $\mathbf{Q}(\zeta_q)$ fixed by automorphisms σ_a for which $a^{n+1} \equiv 1 (\mathrm{mod}\ q)$, and of degree

Received by the editor May 10, 2006 and, in revised form, November 8, 2006.
2000 *Mathematics Subject Classification.* Primary 11L05, 11T24.

$$|\mathbf{Z}_q^{*n+1}| = \begin{cases} \frac{1}{2}\phi(q)/(n+1, \frac{1}{2}\phi(q)) & \text{if } 8|q \text{ and } n \text{ odd}, \\ \phi(q)/(n+1, \phi(q)) & \text{otherwise.} \end{cases} \tag{3}$$

Salie [17] explicitly determined $R(d,q)$ in the classical case $n = 1$ when $p = 2$, and for odd primes p where $q = p^\alpha$ with $\alpha > 1$. Specifically, $R(1,2) = 1$, $R(3,4) = -R(1,4) = 2$; $R(1,8) = R(5,8) = 0$, $R(7,8) = -R(3,8) = 4$; $R(1,16) = R(13,16) = -R(5,16) = -R(9,16) = 4\sqrt{2}$,

$R(d,16) = 0$ if $d \equiv 3 (\text{mod } 4)$;

$R(5,32) = 16\cos(\frac{2\pi}{16} + \frac{\pi}{4})$, $R(d,32) = 0$ if $d \not\equiv 5 (\text{mod } 8)$;

$R(1,64) = 16\sqrt{2}\cos(\frac{2\pi}{32} + \frac{\pi}{4})$, $R(d,64) = 0$ if $d \not\equiv 1 (\text{mod } 8)$;

$R(1,128) = -32\cos(\frac{2\pi}{64} + \frac{\pi}{4})$, $R(d,128) = 0$ if $d \not\equiv 1 (\text{mod } 8)$.

For $\alpha > 5$ ($\alpha \neq 7$), $R(1,2^\alpha) = 2^{(\alpha+3)/2}\cos(\frac{2\pi}{2^{\alpha-1}} + \frac{\pi}{4})$, $R(d,2^\alpha) = 0$ if $d \not\equiv 1 (\text{mod } 8)$. The conjugates $R(d,2^\alpha)$ of $R(1,2^\alpha)$ for $d \equiv 1 (\text{mod } 8)$ with $\alpha > 5$ are determined from (2).

For odd primes p and $\alpha > 1$, $R(1,p^\alpha) = i^{\frac{(p^\alpha-1)^2}{4}} p^{\alpha/2}(\zeta_{p^\alpha}^2 + (\frac{-1}{p})^\alpha \zeta_{p^\alpha}^{-2})$, $R(d,p^\alpha) = 0$ if $(\frac{d}{p}) = -1$. The conjugates $R(d,p^\alpha)$ of $R(1,p^\alpha)$ for $(\frac{d}{p}) = 1$ are determined from (2). Here $(\frac{-}{p})$ denotes the usual Legendre symbol.

Recently [12] I generalized Salie's result to the multi-dimensional case $n > 1$ utilizing the well-known formula [9]

$$R(d,q) = \frac{1}{\phi(q)} \sum_\chi \bar{\chi}(d) G(\chi)^{n+1},$$

the sum over all numerical characters χ modulo q where $G(\chi)$ denotes the classical Gauss sum for the character χ. That treatment relied on Mauclaire's explicit evaluation of $G(\chi)$ for prime powers $q = p^\alpha$ ($\alpha > 1$) and recent results of the author on exponential sums of the form $\sum \chi(x)^{ax} \zeta_q^{bx}$ that used some p-adic methods. Here I give a more elementary evaluation of the multi-dimensional Kloosterman sums (1) using the well-known formulas of Smith [18] (see also Evans [9]), relying on the Galois action (2) and elementary properties of the special exponential sums of the form

$$\sum_{t=1}^{p^\gamma} \zeta_{p^\gamma}^{((1+p^j t)^k - 1 - p^j kt)/p^{\beta+2j}} \qquad (\gamma, j > 0),$$

for suitable exponents $k \equiv 1 (\text{mod } p^\beta)$ when p is odd, and analogous such sums when $p = 2$. I essentially complete the computation that Cochrane, Liu and Zheng [6] initiated in determining upper bounds for such Kloosterman sums.

To best describe the evaluation here, I write $n + 1 = p^\beta u$, for $\beta \geq 0$ and $p \nmid u$, and set $f = \gcd(n+1, p-1)$ if p odd or $f = \gcd(n+1, 2)$ if $p = 2$. For odd primes p, let H denote the group of f-roots of unity modulo $p^{\alpha-\beta}$ (or just modulo p when $\alpha \leq \beta$). I shall show in section 2 for odd primes p with $\alpha > \beta + 1$ that $R(d,q)$ vanishes if $d^{\frac{p-1}{f}} \not\equiv 1 (\text{mod } p^{\beta+1})$, otherwise up to a fourth root of unity is a conjugate of

$$p^{(\alpha n+\beta)/2} \sum_{x \in H} (\frac{x}{p})^c \zeta_{p^{\alpha-\beta}}^x \tag{4}$$

with $c = 0$ or 1 according to whether $\alpha n \equiv \beta (\text{mod } 2)$ or not. I also determine $R(d,p^\alpha)$ for the smaller powers $1 < \alpha \leq \beta + 1$. The important case $R(d,p)$ for odd

primes p remains unresolved. In section 3 I show for $p = 2$ with $\alpha > \beta + 4$ and n odd that $R(d, q)$ vanishes if $d \not\equiv 1 (\mathrm{mod}\ 2^{\beta+2})$, otherwise up to sign is a conjugate of

$$2^{(\alpha n+\beta)/2} \cdot 2\cos(\frac{2\pi}{2^{\alpha-\beta}} + \frac{n\pi}{4}). \tag{5}$$

I separately determine $R(d, 2^\alpha)$ for the smaller powers $\alpha \leq \beta + 4$. The methods may be applied to study certain types of *twisted* Kloosterman sums, but for the sake of simplicity I consider only the ordinary hyper-Kloosterman sums here.

I wish to mention some consequences and related results regarding the explicit values for $R(d, q)$ found here. Expressions (4) and (5) immediately lead to a bound $|R(d, q)| \leq f p^{\frac{\alpha n+\beta}{2}}$ for $\alpha > \beta+1$ ($\alpha > \beta+4$ if $p = 2$), already mentioned in [6], that is a modest improvement of the customary Deligne [7] bound $|R(d, q)| \leq (n+1)p^{\alpha n/2}$ when $\beta > 0$. Moreover, from such expressions (4) and (5), the non-vanishing sums $R(d, q)$ are seen to be integer multiples of ordinary Gauss periods for $p^{\alpha-\beta}$ or a quadratic twist of such. Thus, additional improvement in the upper bound for $|R(d, q)|$ may be obtained using recent estimates for Gauss periods obtained by Bourgain and Chang (chiefly Theorem 4.7 in [4]). When $f > 1$ one may essentially replace f by $fp^{-\epsilon}$ in $|R(d, q)| \leq f p^{\frac{\alpha n+\beta}{2}}$ above, where $\epsilon > 0$ depends on $p^{\alpha-\beta}$ and f. (See also [3] and [14].) These details and the extent to which ϵ can be effectively determined are beyond the scope of the presentation here, but will be discussed elsewhere.

The author has recently studied certain algebraic properties of these Gauss periods and their quadratic twists for prime powers [11] to obtain formulas for the beginning coefficients of their minimal polynomials and associated power sums of zeros. When $f = 2$ a closed form expression for the minimal polynomial and the associated power sums is actually obtained [10]. Those results can be applied with these to describe the polynomial satisfied by the hyper-Kloosterman sums $R(d, q)$ for $d \in \mathbf{Z}_q^*$. This determination may be found in [13].

2. Kloosterman sums for odd prime powers p^α, $\alpha > 1$

As in the introduction I write $n + 1 = p^\beta u$, for $\beta \geq 0$ and $p \nmid u$, and set $f = \gcd(n + 1, p - 1)$. For any $w \not\equiv 0 (\mathrm{mod}\ p)$, let w^{-1} denote the multiplicative inverse of w mod p^α. Let H denote the group of f-roots of unity modulo $p^{\alpha-\beta}$, or just modulo p when $\alpha \leq \beta$, and set $i^* = i^{\frac{(p-1)^2}{4}}$. For any integer d prime to p, one has (chiefly, Cor. 3.2 in [9])

$$R(d, p^\alpha) = p^{ns} \sum_{w=1, w^{n+1} \equiv d (\mathrm{mod}\ p^s)}^{p^s} \zeta_{p^\alpha}^{nw+dw^{-n}} \tag{6}$$

when $\alpha = 2s \geq 2$ is even. For $\alpha = 2s + 1 \geq 3$ odd, one has (chiefly, Cor. 4.2 in [9]) for $\beta = 0$

$$R(d, p^\alpha) = p^{n\alpha/2} \zeta_8^{(1-p)n} (\frac{u}{p}) \sum_{w=1, w^{n+1} \equiv d (\mathrm{mod}\ p^{s+1})}^{p^{s+1}} (\frac{w}{p})^n \zeta_{p^\alpha}^{nw+dw^{-n}}, \tag{7}$$

or for $\beta > 0$

$$R(d, p^\alpha) = p^{(n\alpha+1)/2} \zeta_8^{(1-p)(n+1)} (\frac{d}{p}) \sum_{w=1, w^{n+1} \equiv d (\mathrm{mod}\ p^{s+1})}^{p^s} \zeta_{p^\alpha}^{nw+dw^{-n}}. \tag{8}$$

I note that $nw + dw^{-n}$ is invariant modulo p^α if w is replaced by $w + p^s$ in the sums above in (6) and (8), so that each sum may be taken over any complete set of solutions to the respective congruence up to multiples of p^s.

Before giving the results for Kloosterman sums defined for odd prime powers p^α, I first state an elementary fact about p^γ powers modulo p^α (see also Lemma 2.1 in [6]) and an easy consequence.

Lemma 1. *Let $f > 0$ with $f|(p-1)$. For $\alpha > \gamma \geq 0$, an integer d relatively prime to p is a $p^\gamma f$-power modulo p^α iff d is a $p^\gamma f$ power modulo $p^{\gamma+1}$ iff $d^{\frac{p-1}{f}} \equiv 1 (\mathrm{mod}\ p^{\gamma+1})$.*

Lemma 2. *If $R(d,q) \neq 0$, then $R(d,q)$ is conjugate to $R(d',q)$ for some $d' \equiv 1(\mathrm{mod}\ p^{s'})$ where $s' = [(\alpha+1)/2]$. In addition, if $s' > \beta$, then one may choose $d' = 1$.*

Proof. The hypothesis $R(d,q) \neq 0$ implies that $w_0^{n+1} \equiv d(\mathrm{mod}\ p^{s'})$ for some integer $w_0 \not\equiv 0(\mathrm{mod}\ p)$ from expressions (6) - (8). In particular, $d' \equiv dw_0^{-(n+1)} \equiv 1(\mathrm{mod}\ p^{s'})$ and $R(d,q)$ is conjugate to $R(d',q)$, specifically $R(d,q) = \sigma_{w_0}(R(d',q))$ in (2). If $s' > \beta$, then $d' \equiv 1(\mathrm{mod}\ p^{\beta+1})$ so $d' \in \mathbf{Z}_q^{*n+1}$ by Lemma 1, and thus $R(d,q)$ is conjugate to $R(1,q)$.

The following technical results on exponential sums for prime powers will prove crucial in computing the Kloosterman sums here and later in section 3.

Lemma 3. *Suppose $A(t) = g(t) + p^{r+1}B(t)$ for polynomials $g(t)$ and $B(t)$ with integer coefficients, where p^r is the largest power of the prime p to divide the coefficients of $g'(t)$. Then if $p^{-r}g'(t) \equiv 0(\mathrm{mod}\ p)$ has no solutions, the sum*

$$\sum_{t=1}^{p^\gamma} \zeta_{p^\gamma}^{A(t)} = 0$$

whenever $\gamma \geq r+2$ when p is odd, and $\gamma \geq r+3$ (or $\gamma = 2, r = 0$) when $p = 2$.

The above result can be readily deduced using standard techniques to evaluate exponential sums for prime powers. It is seen to be an immediate consequence of Theorem 2.1 in [5].

For any positive integer $k \equiv 1(\mathrm{mod}\ p)$, say with $k - 1 = p^\beta v$, $p \nmid v$, and any $j > 0$, set

$$H_j(t) = \frac{1}{p^{\beta+2j}}((1+p^j t)^k - 1 - kp^j t). \tag{9}$$

Then it is easy to see that

$$H_j(pt) = p^2 H_{j+1}(t) \tag{10}$$

and for any $\gamma > 1$ and $t \not\equiv 0(\mathrm{mod}\ p)$

$$H_j(t + p^{\gamma-1}) \equiv H_j(t) + 2kvtp^{\gamma-1} \mod p^\gamma. \tag{11}$$

In particular,

Lemma 4. *For any positive β, j, and γ*

$$\sum_{t=1}^{p^\gamma} \zeta_{p^\gamma}^{H_j(t)} = \begin{cases} (\frac{2v}{p}) p^{\frac{\gamma-1}{2}} i^* \sqrt{p} & \text{if } \gamma \text{ odd}, \\ p^{\frac{\gamma}{2}} & \text{if } \gamma \text{ even}, \end{cases}$$

except for $p = 3$ with $\gamma = j = 1$ when

$$\sum_{t=1}^{3} \zeta_3^{H_1(t)} = (\frac{2v}{3}) i\sqrt{3}\zeta_3^v.$$

Proof. First note that $H_j(t) \equiv \frac{v}{2}t^2 \pmod p$ for $j > 1$ or $p > 3$, so $\sum_{t=1}^{p} \zeta_p^{H_j(t)}$ is an ordinary quadratic Gauss sum and the result follows when $\gamma = 1$. For the exceptional case $p = 3$, $\gamma = j = 1$ direct computation yields the value stated above. Now assume $\gamma > 1$ and write $t = ip^{\gamma-1} + l$ for $0 \le i < p$, $1 \le l \le p^{\gamma-1}$. Then

$$\sum_{t=1}^{p^\gamma} \zeta_{p^\gamma}^{H_j(t)} = \sum_{t=1, p\nmid t}^{p^\gamma} \zeta_{p^\gamma}^{H_j(t)} + p \sum_{t=1}^{p^{\gamma-2}} \zeta_{p^{\gamma-2}}^{H_{j+1}(t)}$$

from (10). But the first summand on the right in the above equation is

$$\sum_{t=1, p\nmid t}^{p^\gamma} \zeta_{p^\gamma}^{H_j(t)} = \sum_{i=0}^{p-1} \sum_{l=1, p\nmid l}^{p^{\gamma-1}} \zeta_{p^\gamma}^{H_j(l+ip^{\gamma-1})} = \sum_{l=1, p\nmid l}^{p^{\gamma-1}} \zeta_{p^\gamma}^{H_j(l)} \cdot \sum_{i=0}^{p-1} \zeta_p^{2ikvl} = 0$$

from (11) since $p \nmid kvl$. Thus for $\gamma = 2$, $\sum_{t=1}^{p^2} \zeta_{p^2}^{H_j(t)} = p$, and the general result follows now by induction.

I am now ready to determine the values $R(d, p^\alpha)$ for odd prime powers. I first state the result for even powers p^{2s}. The computation naturally breaks into the cases $\alpha > \beta + 1$ and $2 \le \alpha \le \beta + 1$.

Theorem 1. *Let $q = p^\alpha$ with $\alpha = 2s > \beta + 1$. Then*

$$R(1, q) = p^{(\alpha n+\beta)/2} i^{\frac{(p^\beta-1)^2}{4}} (\frac{-2}{p})^\beta \sum_{x\in H} (\frac{ux}{p})^\beta \zeta_{p^{\alpha-\beta}}^{ux}.$$

The sole exception when $p = 3$ and $\alpha = \beta + 3$ is

$$R(1, 3^\alpha) = 3^{\frac{\alpha}{2}(n+1)-2} i\sqrt{3} \sum_{x\in H} (\frac{ux}{3}) \zeta_{27}^{19ux}.$$

Furthermore, $R(d, q) = 0$ if $d^{\frac{p-1}{f}} \not\equiv 1 (\mathrm{mod}\ p^{\beta+1})$, otherwise $R(d, q)$ is conjugate to $R(1, q)$ above and determined from (2).

Proof. I consider the case $s > \beta$ first. The second assertion of the theorem follows easily in this case from Lemmas 1 and 2. In computing

$$R(1, q) = p^{ns} \sum_{w=1, w^{n+1}\equiv 1 (\mathrm{mod}\ p^s)}^{p^s} \zeta_{p^{2s}}^{nw+w^{-n}}$$

it has been noted that the summation may be taken over any complete set of solutions of the congruence (mod p^s), say those of the form $x(1 + tp^{s-\beta})$ for $1 \le t \le p^\beta$ and x any element of H. One writes $R(1, q) = p^{ns} \sum_{x\in H} S_x$ where

$$S_x = \sum_{t=1}^{p^\beta} \zeta_q^{nx(1+p^{s-\beta}t)+x(1+p^{s-\beta}t)^{-n}}$$

since $x \equiv x^{-n} (\mathrm{mod}\ q)$. Since S_x is the conjugate of S_1 under the action $\zeta_q \to \zeta_q^x$ it suffices to evaluate S_1. Setting $k = (\phi(q)-1)n$ and $j = s - \beta > 0$ one has $k - 1 = p^\beta v$ for $p \nmid v$, and modulo q

$$n + ntp^{s-\beta} + (1+tp^{s-\beta})^{-n} \equiv n + ntp^j + (1+tp^j)^k \equiv n + 1 + (1+p^j t)^k - 1 - kp^j t,$$

so

$$S_1 = \zeta_q^{n+1} \sum_{t=1}^{p^\beta} \zeta_{p^\beta}^{H_j(t)} = \begin{cases} \zeta_q^{n+1} p^{\beta/2} & \text{if } \beta \text{ even}, \\ \zeta_q^{n+1} (\frac{-2u}{p}) i^* \sqrt{p} p^{(\beta-1)/2} & \text{if } \beta \text{ odd} \end{cases}$$

(except $S_1 = \zeta_{81}^{n+1} (\frac{u}{3}) i\sqrt{3}\zeta_3^{2u}$ if $\alpha = 4$ and $\beta = 1$ with $p = 3$) by Lemma 4. This yields the expression for $R(1,q)$ in Theorem 1 whenever $s > \beta$.

Next consider the case $\beta + 1 < \alpha = 2s \le 2\beta$, where from Lemmas 1 and 2 it suffices to consider $R(d,q)$ for $d \equiv 1 (\mathrm{mod}\ p^s)$, say $d = 1 + yp^s$ for some integer y. I assert that if $R(d,q) \neq 0$, then $R(d,q)$ is conjugate to $R(1,q)$, so the second statement of the theorem holds here, too. Indeed, one may choose solutions of $w^{n+1} \equiv d(p^s)$ in (6) of the form

$$\{x(1+pt) | 1 \le t \le p^{s-1}, x \in H\} \tag{12}$$

and write $R(d,q) = p^{ns} \sum_{x \in H} S_x$ where

$$S_x = \sum_{t=1}^{p^{s-1}} \zeta_q^{nx(1+pt) + xd(1+pt)^{-n}}$$

since $x \equiv x^{-n} (\mathrm{mod}\ q)$. Again it suffices to evaluate S_1. With $k = (\phi(q)-1)n$ as before, one finds

$$\begin{aligned} n(1+pt) + d(1+pt)^{-n} &\equiv n + npt + (1+yp^s)(1+pt)^k \\ &\equiv n + 1 + (1+pt)^k - 1 - kpt + yp^s(1+pt)^k \pmod q, \end{aligned}$$

so

$$S_1 = \zeta_q^{n+1+yp^s} \sum_{t=1}^{p^{s-1}} \zeta_{p^{s-1}}^{y((1+pt)^k - 1)/p) + p^{\beta+1-s} H_1(t)} = 0$$

by Lemma 3 when $ord_p\ y < \beta + 1 - s$ since $s \le \beta$ and $g(t) = \frac{1}{p}((1+pt)^k - 1)$ is linear modulo p^{s-1}. Thus if $R(d,q) \neq 0$, then $d \equiv 1 (\mathrm{mod}\ p^{\beta+1})$, and hence d is an $n+1$-power modulo q by Lemma 1 so $R(d,q)$ is conjugate to $R(1,q)$ as asserted. Taking solutions (12) to compute $R(1,q)$ yields $R(1,q) = p^{ns} \sum_{x \in H} S_x$ similarly as before, with

$$\begin{aligned} S_1 = \zeta_q^{n+1} \sum_{t=1}^{p^{s-1}} \zeta_{p^{\alpha-\beta-2}}^{H_1(t)} &= p^{\beta+1-s} \zeta_q^{n+1} \sum_{t=1}^{p^{\alpha-\beta-2}} \zeta_{p^{\alpha-\beta-2}}^{H_1(t)} \\ = p^{\beta+1-s} \zeta_q^{n+1} p^{\frac{\alpha-\beta-2}{2}} \ \text{ or } \ p^{\beta+1-s} \zeta_q^{n+1} (\frac{-2u}{p}) i^* \sqrt{p} p^{\frac{\alpha-\beta-3}{2}} \end{aligned}$$

by Lemma 4 according to whether β is even or odd. The sole exception occurs for $p = 3$ when $\alpha = \beta + 3$ where $S_1 = 3^{\beta+1-s} \zeta_q^{n+1} (\frac{u}{3}) i\sqrt{3}\zeta_3^{2u}$. The expressions for $R(1,q)$ in the statement of the theorem now follows when $\beta + 1 < 2s \le 2\beta$. The proof of the theorem is now complete.

Corollary 1. *If $q = p^{2s}$ and $p \nmid (n+1)$, then*

$$R(1,q) = p^{n\alpha/2} \sum_{x \in H} \zeta_q^{(n+1)x}.$$

For small even values of α one finds that

Proposition 1. *Let $q = p^\alpha$ with $1 < \alpha \leq \beta + 1$ even. For $d \equiv 1 (\mathrm{mod}\ p^{\alpha-1})$,*

$$R(d,p^\alpha) = p^{\frac{\alpha}{2}(n+1)-1} \sum_{x \in H} \zeta_p^{(n+d)x/p^{\alpha-1}},$$

where H is the group of f-roots of unity modulo p. Furthermore $R(d,q) = 0$ if $d^{\frac{p-1}{f}} \not\equiv 1 (\mathrm{mod}\ p^{\alpha-1})$, otherwise $R(d,q)$ is conjugate to some $R(d',q)$ above where $d' \equiv 1 (\mathrm{mod}\ p^{\alpha-1})$ and is determined from (2).

Proof. First assume $d \equiv 1 (\mathrm{mod}\ p^s)$. One may take the solutions of $w^{n+1} \equiv d (\mathrm{mod}\ p^s)$ in formula (6) of the form $w = x(1+tp)$ for $0 \leq t < p^{s-1}$ and $x \in H$. Since $x^{-n} \equiv x (\mathrm{mod}\ q)$, one finds using the negative binomial series that $nx(1+tp) + d(x(1+tp))^{-n}$ is congruent to

$$nx + nxtp + dx(1 - ntp + \binom{n+1}{2} t^2p^2 - \binom{n+2}{3} t^3p^3 + \cdots)$$

$$\equiv (n+d)x + nxtp(1-d) + dx \binom{n+1}{2} t^2p^2 - dx \binom{n+2}{3} t^3p^3 \ (\mathrm{mod}\ p^\alpha).$$

Thus,

$$R(d,p^\alpha) = p^{\frac{\alpha n}{2}} \sum_{x \in H} \zeta_{p^\alpha}^{(n+d)x} \sum_{t=0}^{p^{s-1}-1} \zeta_{p^{\alpha-s-1}}^{nxt\frac{1-d}{p^s}}$$

equals $p^{\frac{\alpha}{2}(n+1)-1} \sum_{x \in H} \zeta_{p^\alpha}^{(n+d)x}$ if $d \equiv 1 (\mathrm{mod}\ p^{\alpha-1})$ and otherwise 0 for $d \equiv 1 (\mathrm{mod}\ p^s)$ since

$$\sum_{t=0}^{p^{s-1}-1} \zeta_{p^{\alpha-s-1}}^{nxt\frac{1-d}{p^s}} = \begin{cases} p^{s-1} & \text{if } d \equiv 1 (\mathrm{mod}\ p^{\alpha-1}), \\ 0 & \text{if } d \not\equiv 1 (\mathrm{mod}\ p^{\alpha-1}). \end{cases}$$

In view of Lemma 2 one has $R(d,p) \neq 0$ if and only if $d \equiv d' w_0^{n+1} (\mathrm{mod}\ p^\alpha)$ with $d' \equiv 1 (\mathrm{mod}\ p^{\alpha-1})$ if and only if d is a $p^\beta f$ power modulo $p^{\alpha-1}$ if and only if $d^{\frac{p-1}{f}} \equiv 1 (\mathrm{mod}\ p^{\alpha-1})$ by Lemma 1. Thus the last statement of the proposition readily follows. This completes the proof of the proposition.

I next consider the case for odd powers p^{2s+1}. □

Theorem 2. *Let $q = p^\alpha$ with $\alpha = 2s+1 > \beta+1$. Then*

$$R(1,q) = p^{(\alpha n+\beta)/2} \zeta_8^{(1-p)(n+1)} (\frac{-2}{p})^{\beta+1} i^{\frac{(p^{\beta+1}-1)^2}{4}} \sum_{x \in H} (\frac{ux}{p})^{\beta+1} \zeta_{p^{\alpha-\beta}}^{ux}.$$

The sole exception is

$$R(1,3^\alpha) = 3^{(\alpha n+\beta)/2} i^{-n} \sum_{x \in H} (\frac{ux}{p}) \zeta_{27}^{19ux}$$

when $p = 3$ and $\alpha = \beta + 3 > 3$. Furthermore, $R(d,q) = 0$ if $d^{\frac{p-1}{f}} \not\equiv 1 (\mathrm{mod}\ p^{\beta+1})$, otherwise $R(d,q)$ is conjugate to $R(1,q)$ above and determined from (2).

Proof. I consider the case $s \geq \beta$ first. The last assertion of the theorem follows in this case as before from Lemmas 1 and 2. When $\beta = 0$ (and hence $u = n+1$) one has from (7) that

$$R(1,q) = p^{\alpha n/2}\zeta_8^{(1-p)n}(\frac{u}{p}) \sum_{w=1,\ w^{n+1}\equiv 1(\mathrm{mod}\ p^{s+1})}^{p^{s+1}} (\frac{w}{p})^n \zeta_{p^\alpha}^{nw+w^{-n}},$$

where the sum may be taken over any complete set of solutions (mod p^{s+1}). Here one may choose w to run through H, so the above becomes

$$R(1,q) = p^{\alpha n/2}\zeta_8^{(1-p)n}(\frac{u}{p})^n \sum_{x\in H} (\frac{x}{p})^n \zeta_{p^\alpha}^{ux},$$

since $x^{-n} \equiv x(\mathrm{mod}\ q)$ for $x \in H$, so $nx + x^{-n} \equiv nx + x \equiv ux(\mathrm{mod}\ q)$. This expression for $R(1,q)$ matches that stated above upon noting $\zeta_8^{1-p} i^* = (\frac{-2}{p})$.

When $\beta \geq 1$, one uses (8) to compute

$$R(1,q) = p^{(\alpha n+1)/2}\zeta_8^{(1-p)(n+1)} \sum_{w=1,\ w^{n+1}\equiv 1(\mathrm{mod}\ p^{s+1})}^{p^s} \zeta_q^{nw+w^{-n}}$$

where the sum may be taken over any complete set of solutions (mod p^s), say those of the form $\{x\cdot(1+p^{s+1-\beta}t)|\ 1 \leq t \leq p^{\beta-1},\ x \in H\}$. One writes

$$R(1,q) = p^{(\alpha n+1)/2}\zeta_8^{(1-p)(n+1)} \sum_{x\in H} S_x,$$

where

$$S_x = \sum_{t=1}^{p^{\beta-1}} \zeta_q^{nx(1+p^{s+1-\beta}t)+x(1+p^{s+1-\beta}t)^{-n}}$$

as before with S_x conjugate to S_1 via the action $\zeta_q \to \zeta_q^x$. To evaluate S_1 again set $k = (\phi(q)-1)n$ with $j = s+1-\beta > 0$. One has $k-1 = p^\beta v$ for $p \nmid v$, and

$$n + np^{s+1-\beta}t + (1+p^{s+1-\beta}t)^{-n} \equiv n+1+(1+p^j t)^k - 1 - kp^j t\ (\mathrm{mod}\ q),$$

so $S_1 = \zeta_q^{n+1}\sum_{t=1}^{p^{\beta-1}} \zeta_{p^{\beta-1}}^{H_j(t)} = \zeta_q^{n+1}p^{(\beta-1)/2}$ or $\zeta_q^{n+1}(\frac{-2u}{p})i^*\sqrt{p}p^{\beta/2-1}$ according to whether $\beta-1$ is even or odd from Lemma 4 (except $S_1 = \zeta_{243}^{n+1}(\frac{u}{3})i\sqrt{3}\zeta_3^{2u}$ if $\alpha = 5$ and $\beta = 2$ with $p = 3$). This yields the expression for $R(1,q)$ whenever $s > \beta > 0$.

Next consider the case $\beta + 1 < \alpha = 2s+1 \leq 2\beta - 1$, where from Lemmas 1 and 2 it suffices to consider $R(d,q)$ for $d \equiv 1(\mathrm{mod}\ p^{s+1})$, say $d = 1 + yp^{s+1}$ for some integer y. I assert that if $R(d,q) \neq 0$, then $R(d,q)$ is conjugate to $R(1,q)$ so the last assertion of the theorem holds for this case, too. Indeed, one may choose solutions of $w^{n+1} \equiv d(\mathrm{mod}\ p^{s+1})$ in (8) of the form

$$\{x(1+pt) \mid 1 \leq t \leq p^{s-1},\ x \in H\ \} \tag{13}$$

and write $R(d,q) = p^{(n\alpha+1)/2}\zeta_8^{(1-p)(n+1)}\sum_{x\in H} S_x$ where

$$S_x = \sum_{t=1}^{p^{s-1}} \zeta_q^{nx(1+pt)+xd(1+pt)^{-n}}$$

since $x^{-n} \equiv x (\mathrm{mod}\ q)$ as before. It suffices to evaluate S_1 with $k = (\phi(q)-1)n$ again. One finds that

$$\begin{aligned} n(1+pt) + d(1+pt)^{-n} &\equiv n + npt + (1+yp^{s+1})(1+pt)^k \\ &\equiv n+1+(1+pt)^k - 1 - kpt + yp^{s+1}(1+pt)^k \ (\mathrm{mod}\ q) \end{aligned}$$

so

$$S_1 = \zeta_q^{n+1+yp^{s+1}} \sum_{t=1}^{p^{s-1}} \zeta_{p^{s-1}}^{y((1+pt)^k-1)/p) + p^{\beta-s}H_1(t)} = 0$$

by Lemma 3 again when $\mathrm{ord}_p y < \beta - s$ similar to before. Thus if $R(d,q) \neq 0$, then $d \equiv 1 (\mathrm{mod}\ p^{\beta+1})$, and hence d is an $n+1$-power modulo q by Lemma 1, so $R(d,q)$ is conjugate to $R(1,q)$ as asserted.

Taking solutions (13) to compute $R(1,q)$ yields

$$R(1,q) = p^{(n\alpha+1)/2} \zeta_q^{(1-p)(n+1)} \sum_{x \in H} S_x,$$

where similar to before

$$S_1 = \zeta_q^{n+1} \sum_{t=1}^{p^{s-1}} \zeta_{p^{\alpha-\beta-2}}^{H_1(t)} = \zeta_q^{n+1} p^{\beta-s} \sum_{t=1}^{p^{\alpha-\beta-2}} \zeta_{p^{\alpha-\beta-2}}^{H_1(t)}$$

equals $\zeta_q^{n+1} p^{\beta-s} p^{(\alpha-\beta-2)/2}$ or $\zeta_q^{n+1} p^{\beta-s} (\frac{-2u}{p}) i^* \sqrt{p} p^{(\alpha-\beta-3)/2}$ by Lemma 4 according to whether β is odd or even. The sole exception occurs for $p=3$ when $\alpha = \beta+3$ where

$$S_1 = \zeta_q^{n+1} 3^{\beta-s} (\frac{u}{3}) i\sqrt{3} \zeta_3^{2u}.$$

The expression for $R(1,q)$ now follows when $\beta+1 < \alpha \leq 2\beta-1$. The proof of the theorem is now complete. □

For small odd values of $\alpha > 1$ one finds

Proposition 2. *Let $q = p^\alpha$ with $3 \leq \alpha \leq \beta+1$ odd.*

For $d \equiv 1 (\mathrm{mod}\ p^{\alpha-1})$,

$$R(d,p^\alpha) = \zeta_8^{(1-p)(n+1)} p^{\frac{\alpha}{2}(n+1)-1} \sum_{x \in H} \zeta_p^{(n+d)x/p^{\alpha-1}},$$

where H is the group of f-roots of unity modulo p. Furthermore, $R(d,p^\alpha) = 0$ if $d^{\frac{p-1}{f}} \not\equiv 1 (\mathrm{mod}\ p^{\alpha-1})$, otherwise $R(d,q)$ is conjugate to some $R(d',q)$ above with $d' \equiv 1 (\mathrm{mod}\ p^{\alpha-1})$ and is determined from (2).

Proof. First assume $d \equiv 1 (\mathrm{mod}\ p^{s+1})$ and choose solutions of $w^{n+1} \equiv d (\mathrm{mod}\ p^{s+1})$ in formula (8) of the form $w = x(1+tp)$ for $0 \leq t < p^{s-1}$ and $x \in H$. Proceeding as in the proof of Proposition 1 one finds

$$\begin{aligned} R(d,p^\alpha) &= p^{\frac{\alpha n+1}{2}} \zeta_8^{(1-p)(n+1)} \sum_{x \in H} \zeta_{p^\alpha}^{(n+d)x} \sum_{t=0}^{p^{s-1}-1} \zeta_{p^{\alpha-s-1}}^{nxt\frac{1-d}{p^s}} \\ &= \zeta_8^{(1-p)(n+1)} p^{\frac{\alpha}{2}(n+1)-1} \sum_{x \in H} \zeta_p^{(n+d)x/p^{\alpha-1}} \end{aligned}$$

if $d \equiv 1 (\mathrm{mod}\ p^{\alpha-1})$ and otherwise is 0 for $d \equiv 1 (\mathrm{mod}\ p^{s+1})$. A similar argument leads to the last statement of the proposition.

Example 1. To illustrate Theorems 1 and 2 and Proposition 2 above, consider the case $n = 6$ for $q = 49, 343$ and 2401. Here $p = 7$ with $\beta = 1$, $u = 1$ and $f = 1$. Proposition 2 applies when $q = 49$ where $s = 1$. Direct calculation using (6) yields $R(1,49) = 7^6\zeta_7$, $R(8,49) = 7^6\zeta_7^2$, $R(15,49) = 7^6\zeta_7^3$, $R(22,49) = 7^6\zeta_7^4$, $R(29,49) = 7^6\zeta_7^5$, $R(36,49) = 7^6\zeta_7^6$ and $R(43,49) = 7^6$, with their conjugates $R(d,49)$ obtained from (2). Here $(\mathbf{Z}_{49}^*)^7 = \{\pm 1, \pm 18, \pm 19\}$, so $R(d,49) \neq 0$ for each $d \in \mathbf{Z}_{49}^*$. For $q = 343$, Theorem 2 applies where $s = 1$ to give $R(1,343) = -7^9 i\sqrt{7}\zeta_{49}$; and for $q = 2401$, Theorem 1 yields $R(1,2401) = -7^{12} i\sqrt{7}\zeta_{343}$ where $s = 2$. In each of these cases, $R(d,q) = 0$ if $d^6 \not\equiv 1 (\mathrm{mod}\ 49)$; otherwise $R(d,q)$ is determined from (2).

3. Kloosterman sums for $q = 2^\alpha$

As before, I write $n + 1 = 2^\beta u$ for $\beta \geq 0$ and u odd, and set $f = \gcd(n+1, 2)$. The following result deals with the case $\beta = 0$.

Proposition 3. *For n even, $R(1,2) = -1$, $R(1,4) = -R(3,4) = (-1)^{n/2} 2^n \zeta_4$, $R(1,8) = 2^{3n/2}\zeta_8^{(-1)^{n/2}}$, $R(1,2^\alpha) = (-1)^{\alpha[\frac{n+2}{4}]} 2^{\alpha n/2} \zeta_{2^\alpha}^{n+1}$ for $\alpha > 3$. In each case, for $d \not\equiv 1 \pmod{2^\alpha}$ with $\alpha \geq 3$, $R(d,2^\alpha)$ is determined from (2).*

Proof. In view of Evans' formulas for $p = 2$ in section 3 and 4 in [9], only the expression for $R(1,2^\alpha)$ for $\alpha = 2s$ with $s > 1$ needs some justification. Here (6) is valid for $p = 2$ too, so

$$R(1,2^{2s}) = 2^{ns} \sum_{0<w<2^s;\ w^{n+1}\equiv 1 (\mathrm{mod}\ 2^s)} \zeta_{2^{2s}}^{nw+w^{-n}}.$$

Since n is even, $w^{n+1} \equiv 1 (\mathrm{mod}\ 2^s)$ has a unique solution $w \equiv 1 (\mathrm{mod}\ 2^s)$, so $R(1,2^{2s}) = 2^{ns}\zeta_{2^{2s}}^{n+1} = 2^{n\alpha/2}\zeta_{2^\alpha}^{n+1}$ in agreement with the statement of the proposition. The last statement follows since $(\mathbf{Z}_{2^\alpha}^*)^{n+1} = \mathbf{Z}_{2^\alpha}^*$ here.

I now assume that $\beta > 0$ throughout the remainder of the section. For any odd integer d where $q = 2^\alpha$ one has (chiefly, Cor. 3.2 in [9])

$$R(d,q) = 2^{ns} \sum_{w=1,\ w^{n+1}\equiv d (\mathrm{mod}\ 2^s)}^{2^s} \zeta_{2^\alpha}^{nw+dw^{-n}} \tag{14}$$

when $\alpha = 2s \geq 2$ is even; whereas for $\alpha = 2s+1 \geq 5$ odd,

$$R(d,q) = (-1)^{\frac{n-1}{4}} 2^{sn+(n+1)/2} \sum_{w=1, 2^s || (w^{n+1}-d)}^{2^s} \zeta_{2^\alpha}^{nw+dw^{-n}} \tag{15}$$

if $\beta = 1$ or

$$R(d,q) = (-1)^{\frac{n+1}{4}} 2^{sn+(n+1)/2} \sum_{w=1, w^{n+1}\equiv d (\mathrm{mod}\ 2^{s+1})}^{2^s} \zeta_{2^\alpha}^{nw+dw^{-n}} \tag{16}$$

if $\beta > 1$.

The case $\alpha \leq 3$ is dealt with in the following result (chiefly from Evans' Theorem 4.3 in [9]).

Proposition 4. *For odd n and d, $R(d,2) = (-1)^{n+1}$, $R(d,4) = (-1)^{\frac{n+d}{2}}2^n$ and*

$$R(d,8) = \begin{cases} 2^{\frac{3n+1}{2}}(\frac{2}{d}) & \text{if } d \not\equiv n(\text{mod } 4), \\ 0 & \text{if } d \equiv n(\text{mod } 4). \end{cases}$$

I begin by stating an elementary fact about 2^γ powers modulo 2^α (see also Lemma 3.2 in [6]) and analogs of Lemmas 1 and 2.

Lemma 5. *For $\gamma > 0$ and $\alpha > \gamma + 1$, an odd integer d is a 2^γ-power modulo 2^α iff d is a 2^γ-power modulo $2^{\gamma+2}$ iff $d \equiv 1(\text{mod } 2^{\gamma+2})$.*

The next fact is an easy consequence of Lemma 5 and Proposition 3.

Lemma 6. *Suppose $\alpha > 3$. If $R(d,q) \neq 0$, then $R(d,q)$ is conjugate to $R(d',q)$ for some $d' \equiv 1(\text{mod } 2^{s'})$, where $s' = [(\alpha+1)/2]$ if α odd and $\beta \neq 1$, otherwise $s' = s$. In addition, if $s' > \beta + 1$, then one may choose $d' = 1$.*

Proof. For $\beta = 0$, each $R(d,2^\alpha) \neq 0$ and is conjugate to $R(1,2^\alpha)$ by Proposition 3, so assume $\beta > 0$. From (14)-(16) the hypothesis $R(d,q) \neq 0$ implies that $w_0^{n+1} \equiv d(\text{mod } 2^{s'})$ for some odd integer w_0. In particular, $d' \equiv dw_0^{-(n+1)} \equiv 1(\text{mod } 2^{s'})$ and $R(d',2^\alpha)$ is conjugate to $R(d,2^\alpha)$, specifically $R(d,q) = \sigma_{w_0}(R(d',q))$ in (2). If $s' > \beta + 1$, then $d' \equiv 1(\text{mod } 2^{\beta+2})$ so $d' \in \mathbf{Z}_q^{*(n+1)}$ by Lemma 5, and thus $R(d,q)$ is conjugate to $R(1,q)$.

For any odd integer k, say with $k - 1 = 2^\beta v$, v odd, and any $j > 0$ set

$$H_j(t) = \frac{1}{2^{\beta-1+2j}}((1+2^j t)^k - 1 - 2^j kt). \tag{17}$$

It is easy to see that

$$H_j(2t) = 4H_{j+1}(t), \tag{18}$$

and for any odd t,

$$H_j(t + 2^{\gamma-1}) \equiv H_j(t) \pmod{2^\gamma} \text{ if } \gamma > 1, \tag{19}$$

$$H_j(t + 2^{\gamma-2}) \equiv H_j(t) + 2^{\gamma-1} \pmod{2^\gamma} \text{ if } \gamma > 3. \tag{20}$$

In particular, one finds the following analog of Lemma 4.

Lemma 7. *For any positive k and γ with k odd and $j > 1$,*

$$\sum_{t=1}^{2^\gamma} \zeta_{2^{\gamma+1}}^{H_j(t)} = (\frac{2}{kv})^\gamma 2^{\gamma/2}\zeta_8^{kv}$$

except for $\gamma = j = 2$ when $\sum_{t=1}^4 \zeta_8^{H_2(t)} = -2\zeta_8^{kv}$.

Proof. I proceed by induction on γ. When $\gamma = 1$ with $j > 1$, $\zeta_4^{H_j(1)} + \zeta_4^{H_j(2)} = \zeta_4^{kv} + 1 = (\frac{2}{kv})\sqrt{2}\zeta_8^{kv}$. Also note for $\gamma = 2$ and $j > 1$,

$$\sum_{t=1}^4 \zeta_8^{H_j(t)} = \zeta_8^{kv+2^j} - 1 + \zeta_8^{kv+2^j} + 1,$$

yielding the statement of the lemma when $\gamma = 2$, including the exceptional value when $j = 2$.

Now assume $\gamma \geq 3$. Then

$$\sum_{t=1}^{2^\gamma} \zeta_{2^{\gamma+1}}^{H_j(t)} = \sum_{t=1, t\ odd}^{2^\gamma} \zeta_{2^{\gamma+1}}^{H_j(t)} + \sum_{t=1}^{2^{\gamma-1}} \zeta_{2^{\gamma-1}}^{H_{j+1}(t)}$$

from (18). I assert that the first sum on the right vanishes. Indeed from (20)

$$\sum_{t=1, t\ odd}^{2^\gamma} \zeta_{2^{\gamma+1}}^{H_j(t)} = \sum_{t=1,\ t\ odd}^{2^{\gamma-1}} (\zeta_{2^{\gamma+1}}^{H_j(t)} + \zeta_{2^{\gamma+1}}^{H_j(t)+2^\gamma}) = \sum_{t=1,\ t\ odd}^{2^{\gamma-1}} (\zeta_{2^{\gamma+1}}^{H_j(t)} - \zeta_{2^{\gamma+1}}^{H_j(t)}) = 0.$$

From (19) the second sum on the right equals

$$2\sum_{t=1}^{2^{\gamma-2}} \zeta_{2^{\gamma-1}}^{H_{j+1}(t)} = 2(\frac{2}{kv})^\gamma 2^{\frac{\gamma-2}{2}} \zeta_8^{kv} = (\frac{2}{kv}) 2^{\gamma/2} \zeta_8^{kv}$$

by the induction hypothesis. This concludes the proof of the lemma.

I am ready to determine the values $R(d, 2^\alpha)$ for $\beta > 0$ and $\alpha > 3$. I first state the result for even powers 2^{2s}. The computation naturally breaks into the cases $\alpha > \beta + 4$ and $4 \leq \alpha \leq \beta + 4$.

Theorem 3. *Let $q = 2^\alpha$ with $\alpha = 2s > \beta + 4 \geq 5$. Then*

$$R(1, q) = (\frac{2}{un})^\beta 2^{\frac{\alpha n+\beta}{2}} (\zeta_{2^{\alpha-\beta}}^{u(1+n2^{\alpha-\beta-3})} + \zeta_{2^{\alpha-\beta}}^{-u(1+n+2^{\alpha-\beta-3})})$$

except

$$R(1, q) = -2^{\frac{\alpha}{2}(n+1)-3} (\zeta_{64}^{u(1+8n)} + \zeta_{64}^{-u(1+8n)})$$

when $\alpha = \beta + 6$. Furthermore, $R(d, q) = 0$ if $d \not\equiv 1 (\mathrm{mod}\ 2^{\beta+2})$, otherwise $R(d, q)$ is conjugate to $R(1, q)$ above and determined from (2).

Proof. I consider the case $s > \beta + 1$ first. The second assertion of the theorem follows in this case from Lemma 6. To compute

$$R(1, q) = 2^{ns} \sum_{w=1, w^{n+1} \equiv 1 (2^s)}^{2^s} \zeta_{2^\alpha}^{nw+w^{-n}}$$

where the summation may be taken over any complete set of solutions (mod 2^s), say those of the form

$$\{\pm(1 + t2^{s-\beta}) |\ 1 \leq t \leq 2^\beta\},$$

one writes $R(1, q) = 2^{ns}(S^+ + S^-)$ where

$$S^\pm = \sum_{t=1}^{2^\beta} \zeta_q^{\pm(n(1+t2^j)+(1+t2^j)^{-n})}$$

with $j = s - \beta \geq 2$. To evaluate S^+, note that

$$n(1+t2^j)+(1+t2^j)^{-n} \equiv n(1+t2^j)+(1+t2^j)^k \equiv n+1+(1+t2^j)^k-1-2^j kt \pmod q$$

where $k = (2^{\alpha-1} - 1)n$ so $k - 1 = 2^\beta v$ with v odd. Then

$$S^+ = \zeta_{2^\alpha}^{n+1} \sum_{t=1}^{2^\beta} \zeta_{2^{\beta+1}}^{H_j(t)} = \zeta_{2^\alpha}^{n+1} (\frac{2}{kv})^\beta 2^{\beta/2} \zeta_8^{kv}$$

(except $S^+ = -2\zeta_{256}^{n+1} \cdot \zeta_8^{kv}$ if $\alpha = 8$ and $\beta = 2$) by Lemma 7. This yields the expression for $R(1,q)$ in Theorem 3 when $s > \beta + 1$.

Next I consider the case $\beta + 4 < \alpha \leq 2\beta + 2$, so $\beta \geq 3$ and $s \geq 4$. By Lemma 6 we may take $d = 1 + \rho 2^s$ for some integer ρ. The solution set for $w^{n+1} \equiv d (\mathrm{mod}\ 2^s)$ in (14) may be chosen as $\{\pm(1+4t) \mid 1 \leq t \leq 2^{s-2}\}$. Then $R(d,q) = 2^{sn}(S^+ + S^-)$ where

$$S^{\pm} = \sum_{t=1}^{2^{s-2}} \zeta_{2^\alpha}^{\pm(n(1+4t)+d(1+4t)^{-n})}.$$

With $k = (2^{\alpha-1} - 1)n$ one has $k - 1 = 2^\beta v$ with v odd, and

$$n(1+4t) + d(1+4t)^{-n} \equiv n(1+4t) + (1+\rho 2^s)(1+4t)^k$$
$$\equiv n + 1\rho 2^s + k\rho 2^{s+2}t + (1+\rho 2^s)((1+4t)^k - 1 - 4kt) \pmod q$$

so

$$S^+ = \zeta_q^{n+1+\rho 2^s} \sum_{t=1}^{2^{s-2}} \zeta_{2^{s-2}}^{k\rho t + (1+\rho 2^s)2^{\beta+1-s}H_2(t)} = 0$$

for $ord_2\rho \ \leq \beta + 1 - s$ by Lemma 3, and similarly for S^-. Thus if $R(d,q) \neq 0$ above, then $d \equiv 1 (\mathrm{mod}\ 2^{\beta+2})$ and $d \in \mathbf{Z}_q^{*n+1}$ so $R(d,q)$ is conjugate to $R(1,q)$. The second assertion of the theorem follows now in this case from Lemmas 5 and 6.

Taking the solutions for $w^{n+1} \equiv 1 (\mathrm{mod}\ 2^s)$ in (14) of the form $\{1 + 2t \mid -2^{s-2} \leq t \leq 2^{s-2} - 1\}$ to compute $R(1,q)$ in this case, one finds $R(1,q) = 2^{sn}(S^+ + S^-)$, where

(21)

$$S^+ = \sum_{t=-2^{s-2},\, t \text{ even}}^{2^{s-2}-2} \zeta_q^{n(1+2t)+(1+2t)^{-n}} \quad \text{and} \quad S^- = \sum_{t=-2^{s-2},\, t \text{ odd}}^{2^{s-2}-1} \zeta_q^{n(1+2t)+(1+2t)^{-n}}.$$

Since n is odd, one notes that S^- becomes

$$S^- = \sum_{t=-2^{s-2},\, t \text{ even}}^{2^{s-2}-1} \zeta_q^{-n(1+2t)-(1+2t)^{-n}},$$

upon replacing t by $-1 - t$ in the expression for S^-. Hence one may write

$$(22) \quad S^+ = \sum_{t'=-2^{s-3}}^{2^{s-3}-1} \zeta_q^{n(1+4t')+(1+4t')^{-n}} \quad \text{and} \quad S^- = \sum_{t'=-2^{s-3}}^{2^{s-3}-1} \zeta_q^{-n(1+4t')-(1+4t')^{-n}}.$$

With $k = (2^{\alpha-1} - 1)n$, one has

$$n(1+4t') + (1+4t')^{-n} \equiv n(1+4t') + (1+4t')^k \equiv n + 1 + 2^{\beta+3}H_2(t') \pmod q,$$

so

$$S^+ = \zeta_q^{n+1} \sum_{t'=-2^{s-3}}^{2^{s-3}-1} \zeta_{2^{\alpha-\beta-3}}^{H_2(t')} = \zeta_q^{n+1} \sum_{t=1}^{2^{s-2}} \zeta_{2^{\alpha-\beta-3}}^{H_2(t)} = \zeta_q^{n+1} 2^{\beta+2-s} \sum_{t=1}^{2^{\alpha-\beta-4}} \zeta_{2^{\alpha-\beta-3}}^{H_2(t)}$$

in view of (19) since $s \leq \beta + 1$. Thus

$$S^+ = (\frac{2}{kv})^\beta 2^{\beta/2} \zeta_q^{n+1} \zeta_8^{kv} = (\frac{2}{nu})^\beta 2^{\beta/2} \zeta_q^{(n+1)(1+n+2^{\alpha-\beta-3})}$$

since $\beta \geq 3$. Similarly, $S^- = (\frac{2}{nu})^\beta 2^{\beta/2}\zeta_q^{-(n+1)(1+n2^{\alpha-\beta-3})}$ so

$$R(1,q) = (\frac{2}{nu})^\beta 2^{\frac{\alpha n+\beta}{2}}(\zeta_{2^{\alpha-\beta}}^{u(1+n2^{\alpha-\beta-3})} + \zeta_{2^{\alpha-\beta}}^{-u(1+n2^{\alpha-\beta-3})}).$$

The sole exception occurs for $\alpha = \beta + 6$, $\beta \geq 4$, when $S^+ = -2^{\beta/2}\zeta_{64}^{u(1+8n)}$ so

$$R(1,q) = -2^{\frac{\alpha}{2}(n+1)-3}(\zeta_{64}^{u(1+8n)} + \zeta_{64}^{-u(1+8n)}).$$

This completes the proof of the theorem.

For small even values α with $\beta > 0$ one finds

Proposition 5. *Let $q = 2^\alpha$ with $\alpha \geq 2$ even. For $\alpha < \beta + 2$,*

$$R(d,q) = \begin{cases} (-1)^{(n+d)/2^{\alpha-1}} 2^{\frac{\alpha}{2}(n+1)-1} & \text{if } d \equiv 1 (\mathrm{mod}\ 2^{\alpha-1}), \\ 0 & \text{otherwise.} \end{cases}$$

For $\alpha = \beta + 2$,

$$R(d,q) = \begin{cases} 0 & \text{if } d \equiv 1 (\mathrm{mod}\ 2^{\alpha-1}) \text{ or } d \not\equiv 1 (\mathrm{mod}\ 2^{\alpha-2}), \\ (-1)^{(n+d)/2^{\alpha-1}} 2^{\frac{\alpha}{2}(n+1)-1} & \text{if } d \equiv 1 + 2^{\alpha-2} \pmod{2^{\alpha-1}}. \end{cases}$$

For $\alpha = \beta + 3$,

$$R(d,q) = \begin{cases} 2^{\frac{\alpha}{2}(n+1)-2}(\zeta_q^{n+d} + \zeta_q^{-(n+d)}) & \text{if } d \equiv 1 (\mathrm{mod}\ 2^{\alpha-2}), \\ 0 & \text{if } d \not\equiv 1 (\mathrm{mod}\ 2^{\alpha-2}). \end{cases}$$

For $\alpha = \beta + 4$,

$$R(d,q) = \begin{cases} 2^{\frac{\alpha}{2}(n+1)-2}(\zeta_q^{n+d} + \zeta_q^{-(n+d)}) & \text{if } d \equiv 1 + 2^{\alpha-3} (\mathrm{mod}\ 2^{\alpha-2}), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. First note that since $s \leq \beta + 2$, $w^{n+1} \equiv 1 (\mathrm{mod}\ 2^s)$ for any odd integer w. Thus from (14) $R(d,q) = 0$ if $d \not\equiv 1 (\mathrm{mod}\ 2^s)$. For $d \equiv 1 (\mathrm{mod}\ 2^s)$, one may choose solutions of $w^{n+1} \equiv d (\mathrm{mod}\ 2^s)$ in (14) of the form $\{\pm(1+4t) \mid 1 \leq t \leq 2^{s-2}\}$. From the negative binomial expansion

$$(1+2x)^{-n} = 1 - n(2x) + \binom{n+1}{2}(2x)^2 - \cdots,$$

one finds

$$n(1+4t) + d(1+4t)^{-n} \equiv n + d + 4tn(1-d) + 2^{\beta+3} t \binom{n+1}{2}(2x)^2 - \cdots \pmod{2^{\beta+4}}.$$

In particular from (14), $R(d,q) = 2^{\frac{\alpha n+1}{2}}(S^+ + S^-)$ where

$$S^\pm = \sum_{t=1}^{2^{s-2}} \zeta_q^{\pm(n+d+4t(1-d)n+2^{\beta+3}t)}.$$

For $\alpha \leq \beta + 3$,

$$S^+ = \zeta_q^{n+d} \sum_{t=1}^{2^{s-2}} \zeta_{2^{s-2}}^{tn(1-d)/2^s} = 2^{s-2}\zeta_q^{n+d}$$

if $d \equiv 1 (\mathrm{mod}\ 2^{\alpha-2})$ and otherwise 0. Similarly $S^- = 2^{s-2}\zeta_q^{-(n+d)}$ or 0 according to whether $d \equiv 1(\mathrm{mod}\ 2^{\alpha-2})$ or not. A routine calculation gives the expressions for $R(d,q)$ for $\alpha \leq \beta+3$ as stated in the proposition. For $\alpha = \beta+4$ above though,

$$S^+ = \zeta_q^{n+d} \sum_{t=1}^{2^{s-2}} \zeta_{2^{s-2}}^{t(n(1-d)/2^s)+2^{s-3})} = 2^{s-2}\zeta_q^{n+d}$$

if $d \equiv 1 + 2^{\beta+1} (\mathrm{mod}\ 2^{\beta+2})$ and otherwise 0. This yields the expression for $R(d,q)$ when $\alpha = \beta+4$.

The analogous situation for odd powers 2^{2s+1} is treated next. The computation again breaks naturally into the cases $\alpha > \beta+4$ and $5 \leq \alpha \leq \beta+4$.

Theorem 4. *Let $q = 2^\alpha$ with $\alpha = 2s+1 > \beta+4 \geq 5$.*

i) *If $\beta = 1$, then*

$$R(1,128) = (-1)^{(n+3)/4} 2^{(7n+1)/2} (\zeta_{64}^{u(1+8n)} + \zeta_{64}^{-u(1+8n)}),$$

$$R(1,q) = (-1)^{(n-1)/4} 2^{(\alpha n+1)/2} (\zeta_{2^{\alpha-1}}^{u(1+n2^{\alpha-4})} + \zeta_{2^{\alpha-1}}^{-u(1+n2^{\alpha-4})}) \text{ for } \alpha > 7.$$

ii) *If $\beta > 1$, then*

$$R(1,q) = (\frac{2}{un})^{\beta-1} (-1)^{(n+1)/4} 2^{(\alpha n+\beta)/2} (\zeta_{2^{\alpha-\beta}}^{u(1+n2^{\alpha-\beta-3})} + \zeta_{2^{\alpha-\beta}}^{-u(1+n2^{\alpha-\beta-3})}),$$

except when $\alpha = \beta+6$, then

$$R(1,q) = (-1)^{(n-3)/4} 2^{\alpha(n+1)/2-3} (\zeta_{64}^{u(1+8n)} + \zeta_{64}^{-u(1+8n)}).$$

Furthermore, $R(d,q) = 0$ if $d \not\equiv 1 (\mathrm{mod}\ 2^{\beta+2})$, otherwise $R(d,q)$ is conjugate to $R(1,q)$ above and determined from (2).

Proof. I consider the case $s > \beta$ first. The last assertion of the theorem follows in this case from Lemma 6. To compute $R(1,q)$ when $\beta = 1$ so $s \geq 3$, one notes that the two solutions of $w^{n+1} \equiv 1 (\mathrm{mod}\ 2^s)$ with $2^s || (w^{n+1}-1)$ in (15) may be take to be $\pm(1+2^{s-1})$. With $k = (2^{\alpha-1}-1)n$ one has $k-1 = 2^\beta v$ with v odd, and $n(1+2^{s-1}) + (1+2^{s-1})^{-n} \equiv n(1+2^{s-1}) + (1+2^{s-1})^k \equiv n+1+\binom{k}{2} 2^{2s-2} (\mathrm{mod}\ 2^\alpha)$ for $s > 3$, so $R(1,q) = (-1)^{\frac{n-1}{4}} 2^{\frac{\alpha n+1}{2}} (\zeta_{2^{\alpha-1}}^{u(1+n2^{\alpha-4})} + \zeta_{2^{\alpha-1}}^{-u(1+n2^{\alpha-4})})$ immediately from (15). When $s = 3$, one readily gets $R(1,128) = -(-1)^{\frac{n-1}{4}} 2^{\frac{\alpha n+1}{2}} (\zeta_{64}^{u(1+8n)} + \zeta_{64}^{-(1+8n)})$ instead.

To compute $R(1,q)$ when $s > \beta > 1$, one may choose solutions of $w^{n+1} \equiv 1 (\mathrm{mod}\ 2^{s+1})$ in (16) of the form $\{\pm(1+2^{s-\beta+1}t) |\ 1 \leq t \leq 2^{\beta-1}\}$, and write $R(1,q) = (-1)^{\frac{n+1}{4}} 2^{\frac{\alpha n+1}{2}} (S^+ + S^-)$, where

$$S^\pm = \sum_{t=1}^{2^{\beta-1}} \zeta_{2^\beta}^{\pm(n(1+2^j t)+(1+2^j t)^{-n})},$$

with $j = s-\beta+1 \geq 2$. To evaluate S^+ note for $k = (2^{\alpha-1}-1)n$ that $n(1+2^j t) + (1+2^j t)^{-n} \equiv n(1+2^j t) + (1+2^j t)^k \equiv n+1+2^{\alpha-\beta} H_j(t) \pmod q$, so

$$S^+ = \zeta_q^{n+1} \sum_{t=1}^{2^{\beta-1}} \zeta_{2^\beta}^{H_j(t)} = \zeta_q^{n+1} (\frac{2}{kv})^{\beta-1} 2^{\frac{\beta-1}{2}} \zeta_8^{kv}$$

(except $S^+ = -2\zeta_{512}^{n+1}\zeta_8^{kv}$ if $\alpha = 9$ and $\beta = 3$) by Lemma 7 as before. This yields the desired expression for $R(1,q)$ in ii).

Next consider the case $\beta+5 \le \alpha \le 2\beta+1$ so $\beta \ge s \ge 4$. By Lemma 6 we may take $d = 1+\rho 2^{s+1}$ for some integer ρ. The solution set for $w^{n+1} \equiv d (\mathrm{mod}\ 2^{s+1})$ in (16) may be chosen as $\{\pm(1+4t) \mid 1 \le t \le 2^{s-2}\}$ with $R(d,q) = (-1)^{\frac{n+1}{4}} 2^{\frac{\alpha n+1}{2}} (S^+ + S^-)$ where

$$S^{\pm} = \sum_{t=1}^{2^{s-2}} \zeta_q^{\pm(n(1+4t)+d(1+4t)^{-n})}.$$

Now one gets similarly as before that

$$S^+ = \zeta_q^{n+1+\rho 2^{s+1}} \sum_{t=1}^{2^{s-2}} \zeta_{2^{s-2}}^{k\rho t + (1+\rho 2^{s+1}) 2^{\beta-s} H_2(t)} = 0$$

for $ord_2\ \rho \le \beta - s$ by Lemma 3, and also for S^-. Thus if $R(d,q) \ne 0$ here, $d \equiv 1 (\mathrm{mod}\ 2^{\beta+2})$ so $R(d,q)$ is conjugate to $R(1,q)$ again as asserted in the last statement of the theorem.

To compute $R(1,q)$ using (16) one may choose $w^{n+1} \equiv 1 (\mathrm{mod}\ 2^{s+1})$ of the form $\{1+2t \mid -2^{s-2} \le t \le 2^{s-2}-1\}$. One has $R(1,q) = (-1)^{\frac{n+1}{4}}\ 2^{\frac{\alpha n+1}{2}}\ (S^+ + S^-)$, with S^+ and S^- as in (21) and (22). Once again one finds

$$S^+ = \zeta_q^{n+1} \sum_{t'=-2^{s-3}}^{2^{s-3}-1} \zeta_{2^{\alpha-\beta-3}}^{H_2(t')} = \zeta_q^{n+1} 2^{\beta+1-s} \sum_{t=1}^{2^{\alpha-\beta-4}} \zeta_{2^{\alpha-\beta-3}}^{H_2(t)}$$

$$= (\frac{2}{nu})^{\beta-1} 2^{\frac{\beta-1}{2}} \zeta_q^{n+1} \zeta_8^{kv} = (\frac{2}{nu})^{\beta-1} 2^{\frac{\beta-1}{2}} \zeta_q^{(n+1)(1+n2^{\alpha-\beta-3})}$$

since $\beta \ge s \ge 4$; and similarly, $S^- = (\frac{2}{nu})^{\beta-1} 2^{\frac{\beta-1}{2}} \zeta_q^{-(n+1)(1+n2^{\alpha-\beta-3})}$. Thus

$$R(1,q) = (-1)^{\frac{n+1}{4}} 2^{\frac{\alpha n+\beta}{2}} (\zeta_{2^{\alpha-\beta}}^{u(1+n2^{\alpha-\beta-3})} + \zeta_{2^{\alpha-\beta}}^{-u(1+n2^{\alpha-\beta-3})}).$$

The sole exception occurs for $\alpha = \beta+6$, $\beta \ge 5$ when $S^+ = -2^{\frac{\beta-1}{2}} \zeta_{64}^{u(1+8n)}$ so

$$R(1,q) = -(-1)^{\frac{n+1}{4}} 2^{\frac{\alpha}{2}(n+1)-3} (\zeta_{64}^{u(1+8n)} + \zeta_{64}^{-u(1+8n)}).$$

The proof of the theorem is now complete.

For small odd values of α with $\beta > 0$ one finds here that

Proposition 6. *Let $q = 2^\alpha$ with $\alpha > 3$ odd. For $\alpha < \beta + 2$,*

$$R(d,q) = \begin{cases} (-1)^{(n+d)/2^{\alpha-1}} 2^{\frac{\alpha}{2}(n+1)-1} & \text{if } d \equiv 1 (\mathrm{mod}\ 2^{\alpha-1}), \\ 0 & \text{otherwise.} \end{cases}$$

For $\alpha = \beta + 2$,

$$R(d,q) = \begin{cases} 0 & \text{if } d \equiv 1 (\mathrm{mod}\ 2^{\alpha-1}) \text{ or } d \not\equiv 1 (\mathrm{mod}\ 2^{\alpha-2}), \\ (-1)^{(n+d)/2^{\alpha-1}} 2^{\frac{\alpha}{2}(n+1)-1} & \text{if } d \equiv 1 + 2^{\alpha-2} (\mathrm{mod}\ 2^{\alpha-1}). \end{cases}$$

For $\alpha = \beta + 3$,

$$R(d,q) = \begin{cases} (-1)^{\frac{n+1}{4}} 2^{\frac{\alpha}{2}(n+1)-2} (\zeta_q^{n+d} + \zeta_q^{-(n+d)}) & \text{if } d \equiv 1 (\mathrm{mod}\ 2^{\alpha-2}), \\ 0 & \text{if } d \not\equiv 1 (\mathrm{mod}\ 2^{\alpha-2}). \end{cases}$$

For $\alpha = \beta + 4$,

$$R(d,q) = \begin{cases} (-1)^{\frac{n+1}{4}} 2^{\frac{\alpha}{2}(n+1)-2}(\zeta_q^{n+d} + \zeta_q^{-(n+d)}) & \text{if } d \equiv 1 + 2^{\alpha-3} \pmod{2^{\alpha-2}}, \\ 0 & \text{otherwise.} \end{cases}$$

The sole exception occurs for $\beta = 1$ *where*

$$R(d,32) = \begin{cases} (-1)^{\frac{n-1}{4}} 2^{\frac{5n+1}{2}}(\zeta_{32}^{n+d} + \zeta_{32}^{-n-d}) & \text{if } d \equiv 5 \pmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Here $\beta > 1$ (except as noted last) and $s+1 \leq \beta+2$ so $w^{n+1} \equiv 1 \pmod{2^{s+1}}$ for any odd integer w. Thus from (16) $R(d,q) = 0$ if $d \not\equiv 1 \pmod{2^{s+1}}$. For $d \equiv 1 \pmod{2^{s+1}}$ one may choose solutions of $w^{n+1} \equiv d \pmod{2^{s+1}}$ in (16) of the form $\{\pm(1+4t) \mid 1 \leq t \leq 2^{s-2}\}$. The proof proceeds as that for Proposition 5 to obtain the expressions for $R(d,q)$ as stated in the proposition, including the exceptional case $\alpha = 5$, $\beta = 1$ using (15).

I conclude with an example illustrating Theorems 3 and 4 and Propositions 5 and 6 above.

Example 2. Consider the case $n = 3$ with $q = 32, 64, 128$ and 256. Here $\beta = 2$ with $u = 1$ and $f = 2$. Direct calculation using (16) yields $R(1,32) = -R(17,32) = -256\sqrt{2}$ and $R(9,32) = -R(25,32) = 256\sqrt{2}$. The values $R(d,32) = 0$ for $d \not\equiv 1 \pmod 8$. This is in agreement with the values given in Proposition 6. Also from (14), one obtains as expected from Proposition 5 that $R(9,64) = 2^{11} \cos \frac{3\pi}{8}$ with $R(d,64)$ conjugate to $R(9,64)$ if $d \equiv 9 \pmod{16}$ and otherwise equals 0. Theorem 4 applies when $q = 128$. Here one finds $R(1,128) = 2^{12}\sqrt{2}\cos \frac{13\pi}{16}$ with conjugates $R(d,128)$ for $d \equiv 1 \pmod{16}$ determined from (2). If $d \not\equiv 1 \pmod{16}$, $R(d,128) = 0$. Theorem 3 applies when $q = 256$ where $s = 4$. From (14) one obtains $R(1,256) = 2^{14} \cos \frac{7\pi}{32}$ as expected, with conjugates $R(d,256)$ for $d \equiv 1 \pmod{16}$ determined from (2). If $d \not\equiv 1 \pmod{16}$, $R(d,256) = 0$.

Using Smith's [9, 18] formulas, I have tabulated below the non-zero values $R(d,q)$, one for each $n+1$-st power class modulo q, for several small values of n and small powers $q = p^\alpha$ ($\alpha > 1$) with $\beta > 0$. The explicit calculations confirm the values obtained from Theorems 1-4 and Propositions 2, 5 and 6.

$n = 2 : R(1,9) = 9\zeta_3$; $R(4,9) = 9\zeta_3^2$; $R(7,9) = 9$ with $\mathbf{Z}_9^{*3} = \{\pm 1\}$
$R(1,27) = 27\zeta_9 i\sqrt{3}$ with $\mathbf{Z}_{27}^{*3} = \{\pm 1, \pm 8, \pm 10\}$
$R(1,81) = 81\zeta_{27}^{19} i\sqrt{3}$ with $\mathbf{Z}_{81}^{*3} = \{x | x \equiv \pm 1 \pmod 9\}$
$n = 3 : R(1,4) = -R(3,4) = 8$; $R(1,8) = -R(5,8) = 32$; $R(5,16) = -R(13,16) = -128$
$R(1,32) = -R(9,32) = -256\sqrt{2}$ with $\mathbf{Z}_{32}^{*4} = \{1, 17\}$
$R(9,64) = 2^{11}\cos(3\pi/8)$ with $\mathbf{Z}_{64}^{*4} = \{1, 17, 33, 49\}$
$R(1,128) = 2^{12}\sqrt{2}\cos(13\pi/16)$ with $\mathbf{Z}_{128}^{*4} = \{x | x \equiv 1 \pmod{16}\}$
$R(1,256) = 2^{14}\cos(7\pi/32)$ with $\mathbf{Z}_{256}^{*4} = \{x | x \equiv 1 \pmod{16}\}$
$n = 5 : R(3,4) = -R(1,4) = 32$; $R(7,8) = -R(3,8) = 256$; $R(1,16) = R(5,16) = -2^{10}\sqrt{2}$
$R(5,32) = -2^{14}\cos(5\pi/8)$ with $\mathbf{Z}_{32}^{*2} = \{1, 9, 17, 25\}$
$R(1,64) = 2^{16}\sqrt{2}\cos(\pi/16)$ with $\mathbf{Z}_{64}^{*2} = \{x | x \equiv 1 \pmod 8\}$
$R(1,128) = -2^{19}\cos(27\pi/32)$ with $\mathbf{Z}_{128}^{*2} = \{x | x \equiv 1 \pmod 8\}$
$R(1,9) = R(7,9) = -243$, $R(4,9) = 486$;

$R(1,27) = -2 \cdot 3^8 \cos(4\pi/9)$ with $\mathbf{Z}_{27}^{*6} = \{1, 10, 19\}$
$R(1,81) = 2 \cdot 3^{10}\sqrt{3}\sin(22\pi/27))$ with $\mathbf{Z}_{81}^{*6} = \{1, 10, 19, 28, 37, 46, 55, 64, 73\}$
$n = 7 : R(1,4) = -R(3,4) = 128$; $R(1,8) = -R(5,8) = 2^{11}$; $R(1,16) = -R(9,16) = -2^{15}$; $R(25,32) = -R(9,32) = 2^{19}$;
$R(1,64) = -R(17,64) = 2^{22}\sqrt{2}$ with $\mathbf{Z}_{64}^{*8} = \{1, 33\}$
$R(17,128) = 2^{27}\cos(3\pi/8)$ with $\mathbf{Z}_{128}^{*8} = \{1, 33, 65, 97\}$
$R(1,256) = 2^{30}\sqrt{2}\cos(3\pi/16)$ with $\mathbf{Z}_{256}^{*8} = \{x | x \equiv 1 (\mathrm{mod}\ 32)\}$
$R(1,512) = -2^{34}\cos(7\pi/32)$ with $\mathbf{Z}_{512}^{*8} = \{x | x \equiv 1 (\mathrm{mod}\ 32)\}$
$n = 8 : R(1,9) = 3^8$, $R(4,9) = 3^8\zeta_3$, $R(7,9) = 3^8\zeta_3^2$ with $\mathbf{Z}_9^{*3} = \{\pm 1\}$
$R(1,27) = -3^{12}i\sqrt{3}\zeta_3$, $R(10,27) = -3^{12}i\sqrt{3}\zeta_3^2$, $R(19,27) = -3^{12}i\sqrt{3}$ with $\mathbf{Z}_{27}^{*9} = \{\pm 1\}$
$R(1,81) = 3^{17}\zeta_9$ with $\mathbf{Z}_{81}^{*9} = \{\pm 1, \pm 28, \pm 55\}$
$R(1,243) = 3^{21}\zeta_{27}^{19}$ with $\mathbf{Z}_{243}^{*9} = \{x | x \equiv \pm 1 (\mathrm{mod}\ 27\}$
$n = 9 : R(3,4) = -R(1.4) = 2^9$; $R(7,8) = -R(3,8) = 2^{14}$
$R(1,16) = -R(5,16) = -2^{18}\sqrt{2}$ with $\mathbf{Z}_{16}^{*2} = \{1, 9\}$
$R(5,32) = 2^{24}\cos(7\pi/8)$ with $\mathbf{Z}_{32}^{*2} = \{1, 9, 17, 25\}$
$R(1,64) = -2^{28}\sqrt{2}\cos(7\pi/16)$ with $\mathbf{Z}_{64}^{*2} = \{x | x \equiv 1 (\mathrm{mod}\ 8)\}$
$R(1,128) = 2^{33}\cos(13\pi/32)$ with $\mathbf{Z}_{128}^{*2} = \{x | x \equiv 1 (\mathrm{mod}\ 8)\}$
$R(1,25) = R(6,25) = R(14,25) = R(4,25) = 5^9 \cdot 2cos(4\pi/5)$; $R(16,25) = 2 \cdot 5^9$ with $\mathbf{Z}_{25}^{*10} = \{\pm 1\}$

References

[1] B.C. Berndt, R.J. Evans and K.S. Williams, *Gauss and Jacobi Sums*, Wiley-Interscience, New York, (1998). MR1625181 (99d:11092)
[2] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, (1966). MR0195803 (33:4001)
[3] J. Bourgain, "Exponential sum estimates on subgroups of $\mathbf{Z}_q^*$, q arbitrary," J. Analyse Math. 97 (2005), 317-355.
[4] J. Bourgain and M-C. Chang, "Exponential sum estimates over subgroups and almost subgroups of $\mathbf{Z}_q^*$, where q is composite with few prime factors", Geom. Funct. Anal. 16 (2006), 327–366. MR2231466 (2007d:11093)
[5] T. Cochrane and Z. Zheng, "Pure and mixed exponential sums," Acta Arith. 91 no. 3 (1999), 249-278. MR1735676 (2000k:11093)
[6] T. Cochrane, M. Liu and Z. Zheng, "Upper bounds on n-dimensional Kloosterman sums," J. Number Theory 106 (2004), 259-274. MR2059074 (2005d:11122)
[7] P. Deligne, "Applications de la formula des traces aux sommes trigonometriques" in *Cohomologie etale* (SGA 4.5), 168-232, *Lecture Notes in Math. 569*, Springer-Verlag, Berlin (1977).
[8] W. Duke, "On multiple Salie sums", Proc. Amer. Math Soc. 114 (1992), 623-625. MR1077785 (92f:11113)
[9] R.J. Evans, "Twisted Hyper-Kloosterman Sums over finite rings of integers", in *Proc. Millennial Conf. No. Theory, vol I*, 429 -449; M.A. Bennett et al. eds, A.K. Peters, Natick, MA (2002). MR1956239 (2003m:11125)
[10] S. Gurak, "Minimal polynomials for Gauss periods with $f = 2$", Acta Arith. 121, no. 3 (2006), 233-257. MR2218343 (2006m:11119)
[11] S. Gurak, "On the minimal polynomial of Gauss periods for prime powers", Math Comp. 75 (2006), 2021-2035. MR2240647
[12] S. Gurak, "Explicit values of multi-dimensional Kloosterman sums for prime powers, I" (to appear)
[13] S. Gurak, "Polynomials for Hyper-Kloosterman sums" (to appear)
[14] D.R. Heath-Brown and S. Konyagan, "New bounds for Gauss sums derived from k-th powers and for Heilbron's Exponential Sum," Quat. J. Math. 51 (2000), 221-235. MR1765792 (2001h:11106)

[15] H. Iwaniec, *Topics in classical automorphic forms* Graduate Studies in Mathematics, 17, American Mathematical Society, Providence, RI (1997). MR1474964 (98e:11051)
[16] H.D. Kloosterman, "On the representation of a number in the form $ax^2 + by^2 + cz^2 + dt^2$", Acta Math. 49 (1926), 407-464.
[17] H. Salie, "Uber die Kloostermanschen Summen $S(u, v : q)$", Math. Z. 34 (1932), 91-109. MR1545243
[18] R.A. Smith, "On n-dimensional Kloosterman sums", J. Number Theory 11 (1979), 324-343. MR544261 (80i:10052)

Department of Mathematics, University of San Diego, San Diego, California 92110