ON JACOBI FUNCTIONS

EMMA LEHMER
The Jacobi functions\(^1\) \(R_m\) are usually defined by

\[
R_m = R_m^x(a) = \sum_{s=1}^{p-2} \alpha^{\text{ind } s} = -\left(\frac{s + 1}{a}\right) \text{ind } s + 1
\]

where \(\alpha = e^{2\pi i/k}\) and \(\text{ind } s = \text{ind}_s s\) is taken with respect to some primitive root \(g\) of a prime \(p = kn + 1\). Therefore \(R_m\) depends in general on the choice of primitive root and all the explicit results which have been given for special cases, as in [1], [2], [7] and others contain ambiguities of sign due to this indeterminancy. In a recent work on power character matrices [4] it became necessary to make the known results more explicit and to obtain some new ones. It is the purpose of this note to give explicit results in case 2 is not a \(k\)th power residue of \(p\) for \(k = 3, 4, 5\) and 6 and for all \(m\). The case in which 2 is a \(k\)th power residue of \(p\) still remains ambiguous.

We find it more convenient to use the character notation

\[
\chi(h) = \chi(h) = \begin{cases} 
\alpha^{\text{ind } h} & \text{if } (h, p) = 1 \\
0 & \text{otherwise}
\end{cases}
\]

in order to make use of all the multiplicative properties of the characters. In this notation \(R_m\) becomes

\[
R_m = \sum_{s=1}^{p-2} \chi(s) \chi(s + 1)^{-m-1}.
\]

The following relations are well-known and can be easily derived from the definition as in [4].

\[
R_m = \chi(-1)R_{k-1-m} = \chi(-1) \sum_{s=1}^{p-2} \chi(s) \chi(s + 1)
\]

\[
R_{k-1} = -\chi(-1) = (-1)^{m+1}.
\]

We shall need three other relations which we proceed to prove.

**Lemma 1.** If \(k\) is odd, then

\[
R_s(\alpha) = R_s(\alpha^k) \text{ for } k = 2^\lambda + 1
\]

**Proof.** Let \(s\tilde{s} = 1 \pmod{p}\) Then

\end{document}
LEMMA 2. If $k$ is even, then

$$R_{\mu} = \chi(4)R_{1}, \text{ where } k = 2\mu.$$  

Proof. Using (4)

$$R_{\mu} = \chi(-1) \sum_{s=1}^{p-2} \chi(s)\chi(s+1) = \chi(-1) \sum_{s=1}^{p-2} \chi(s)\chi(s+1)$$

$$= \chi(-1) \left[ \sum_{s=1}^{p-2} \chi(s)[1 + \chi(s+1)] - \sum_{s=1}^{p-2} \chi(s) \right].$$

If $s + 1$ is not a square, then the expression in the square brackets vanishes. Letting $s + 1 = t^2$ we obtain

$$R_{\mu} = \chi(-1) \left[ \sum_{t=1}^{p-1} \chi(t^2 - 1) + \chi(-1) \right] = \chi(-1) \sum_{t=0}^{p-1} \chi(t^2 - 1).$$

Now let $t = 2s + 1$, then

$$R_{\mu} = \chi(-4) \sum_{t=1}^{p-2} \chi(s)\chi(s+1) = \chi(4)R_{1}.$$

LEMMA 3. If $k$ is oddly even, then

$$R_{k}^{(b)}(\alpha) = \chi_{2\nu+1}(4)R_{k}^{(2\nu+1)}(\beta) \text{ where } k = 4\nu + 2, \text{ and } \beta = \alpha^2.$$  

Proof.

$$R_{k}^{(b)}(\alpha) = \sum_{s=1}^{p-2} \chi(s)\chi^{2\nu+1}(s + 1) = \sum_{s=1}^{p-2} \chi(s)\chi^{2\nu+1}(s + 1)$$

$$= \sum_{s=1}^{p-2} \chi^{2\nu+1}(s)\chi^{2\nu+2}(s + 1) = \sum_{s=1}^{p-2} \chi(s)\chi^{2\nu+2}(s + 1)$$

$$= \sum_{s=1}^{p-2} \chi_{2\nu+1}(s)\chi(s + 1)$$

$$= \sum_{s=1}^{p-2} \chi_{2\nu+1}(s)[1 + \chi(s + 1)] - \sum_{s=1}^{p-2} \chi_{2\nu+1}(s).$$

Letting $s + 1 = t^2$ as before:

$$R_{k}^{(b)}(\alpha) = \sum_{t=1}^{p-2} \chi_{2\nu+1}(t^2 - 1) = \chi_{2\nu+1}(4) \sum_{s=1}^{p-2} \chi_{2\nu+1}(s)\chi_{2\nu+1}(s + 1)$$

$$= \chi_{2\nu+1}(4)R_{1}^{(2\nu+1)}(\beta^2)$$

$$= \chi_{2\nu+1}(4)R_{1}^{(2\nu+1)}(\beta)$$
by Lemma 1.
But by (4) and Lemma 2:
\[ R_{2
u+1} = \chi(-1)R_{2
u} = \chi_{k}(4)R_{1} , \quad k = 4\nu + 2 . \]
Hence by Lemma 3:
\[ (9) \quad R_{2
u}^{(\nu)}(\alpha) = \chi_{k}(-4)R_{2\nu+1}^{(\nu)}(\beta) = \chi_{k}(-4)R_{1}^{(\nu+1)}(\beta) \]
Armed with these relations we can express all the Jacobi functions for \( k = 3, 4, 5 \) and 6 in terms of the corresponding \( R_{i} \) as follows.

\[ k = 3, \quad R_{2} = -1 \]
\[ k = 4, \quad R_{3} = -\chi(-1), \quad R_{4} = \chi(-1)R_{1} \text{ by (3)} \]
\[ k = 5, \quad R_{4} = -1, \quad R_{5} = R_{1} \text{ by (3) and } R_{2} = R_{1}(\alpha^{2}) \text{ by Lemma 1.} \]
\[ k = 6, \quad R_{5} = -\chi(-1). \quad R_{4} = \chi(-1)R_{1} \text{ and } R_{2} = \chi(-1)R_{3} \text{ by (3).} \]

By Lemma 2, however, \( R_{3} = \chi(4)R_{1} \) and hence \( R_{2} = \chi(-4)R_{1} \). Moreover by (9) \( R_{1}^{(6)} = \chi(-4)R_{1}^{(3)} \), so that it is sufficient to determine \( R_{1} \) for \( k = 3 \) in order to determine all the \( R_{i} \)'s for \( k = 3 \) and \( k = 6 \).

We now proceed to expand \( R_{i} \) in powers of \( \alpha \). If we write
\[ R_{i} = \chi(-1)\sum_{s=1}^{p-1} \chi(s)\chi(s+1) = \chi(-1)\sum_{v=0}^{k-1} a_{v}\alpha^{v} \]
then \( a_{v} \) is the number of solutions of
\[ s^{2} + s = g^{vt+v} \quad (t = 0, 1, \cdots, n - 1) \]
and is given by
\[ a_{v} = \sum_{v=0}^{k-1} \sum_{t=0}^{n-1} [1 + \chi(1 + 4g^{vt+v})] . \]
Hence
\[ R_{i} = \chi(-1)\sum_{v=0}^{k-1} \sum_{t=0}^{n-1} \chi_{k}(1 + 4g^{vt+v})\alpha^{v} \]
\[ = \frac{\chi(-1)}{k} \sum_{v=0}^{k-1} \sum_{t=1}^{n-1} \chi_{k}(1 + 4x^{t}g^{v})\alpha^{v} \]
\[ = \frac{\chi(-1)}{k} \sum_{v=0}^{k-1} \alpha^{v} \sum_{t=0}^{n-1} \chi_{k}(4g^{v})\chi_{s}(x^{k} + (4g^{v})) \]
\[ = \frac{\chi(-1)}{k} \sum_{v=0}^{k-1} \chi_{k}(4g^{v})\psi_{k}(4g^{v}) \]
where [5]
\[ \psi_{k}(D) = \sum_{x=1}^{n-1} \chi_{s}(x^{k} + D) = \begin{cases} \left( \frac{D}{P} \right) \psi_{k}(D) & \text{if } k \text{ is even} \\ \left( \frac{D}{P} \right) \varphi_{k}(D) & \text{if } k \text{ is odd} \end{cases} \]
and
\[ \varphi_k(D) = \sum_{x=1}^{\frac{k-1}{2}} \chi_2(x) \chi_3(x^k + D) = -\left( \frac{D}{p} \right) \varphi_{k}(D), \ k \text{ even} \]
is the well-known Jacobsthal [3] function. Hence

\[ R_1 = \begin{cases} \frac{\chi(-1)}{k} \sum_{v=0}^{\frac{k-1}{2}} \varphi_k(4g^v)\alpha^v & \text{if } k \text{ is even} \\ \frac{1}{k} \sum_{v=0}^{\frac{k-1}{2}} \varphi_k(4g^v)\alpha^v & \text{if } k \text{ is odd} . \end{cases} \]

Making use of the relations [5]

\[ \varphi_k(m^kD) = \chi_{k+1}(m)\varphi_k(D) \quad (11) \]
\[ \psi_k(m^kD) = \chi_k(m)\psi_k(D) \quad (12) \]
and

\[ \psi_{2k}(D) = \psi_k(D) + \varphi_k(D) \quad (13) \]

we have for \( k \) even, substituting (13) into (10)

\[ R_1 = \frac{\chi(-1)}{k} \left[ \sum_{v=0}^{\frac{k-1}{2}} \psi_{k/2}(4g^v)\alpha^v + \sum_{v=0}^{\frac{k-1}{2}} \varphi_{k/2}(4g^v)\alpha^v \right] . \]

By (11) and (12)

\[ R_1 = \begin{cases} \frac{2\chi(-1)}{k} \sum_{v=0}^{\frac{k-1}{2}} \varphi_{k/2}(4g^v)\alpha^v & \text{if } k/2 \text{ is odd} \\ \frac{2\chi(-1)}{k} \sum_{v=0}^{\frac{k-1}{2}} \varphi_{k/2}(4g^v)\alpha^v & \text{if } k/2 \text{ is even} . \end{cases} \]

Since the functions \( \varphi \) and \( \psi \) have been unequivocally determined by us in [5] and [6] for \( k = 3, 4, 5 \) and 6 in case 2 is not a \( k \)th power residue we can apply these results directly to the determination of the corresponding \( R_i \). For \( k = 3 \) let \( p = A^2 + 3B^2 = 3n + 1, A \equiv B \equiv 1 \pmod{3} \).

By (10)

\[ R_1 = \frac{1}{3} [\varphi_3(4g) + \omega \varphi_3(4g) + \omega^2 \varphi_3(4g^3)] . \]

By [6]

\[ \varphi_3(D) = \begin{cases} -(2A + 1) & \text{if } D \equiv u^3 \pmod{p} \\ A - 3B - 1 & \text{if } D \equiv 2u^3 \pmod{p} \\ A + 3B - 1 & \text{if } D \equiv 4u^3 \pmod{p} . \end{cases} \]
Hence

\[ R_1 = \begin{cases} 
\frac{1}{3} [(A + 3B - 1) - (2A + 1)\omega + (A - 3B - 1)\omega^2] & \text{if ind } 2 \equiv 1 \pmod{3} \\
\frac{1}{3} [(A + 3B - 1) - (A - 3B - 1)\omega - (2A + 1)\omega^2] & \text{if ind } 2 \equiv 2 \pmod{3}
\end{cases} \]

or

\[ R_1 = \begin{cases} 
2B + (B - A)\omega & \text{if ind } 2 \equiv 1(3) \text{ or if } \chi_3(2) = \omega \\
2B + (B - A)\omega^2 & \text{if ind } 2 \equiv 2(3) \text{ or if } \chi_3(2) = \omega^2.
\end{cases} \]

Hence if \( \chi(2) \neq 1 \), then

\[ R_1 = 2B + (B - A)\chi_3(2), \quad A \equiv B \equiv 1 \pmod{3}. \quad (15) \]

If 2 is a cubic residue, \( B \equiv 0 \pmod{3} \) and the sign of \( B \) is not determined. However

\[ R_1 = \frac{1}{3} [\varphi_3(1) + \varphi_3(g)\omega + \varphi_3(g^2)\omega^2] \]

\[ = \frac{1}{3} [-(2A + 1) + (A \pm 3B - 1)\omega + (A \mp 3B - 1)\omega^2] \]

\[ = -A \pm B(\omega - \omega^2) = (-A \pm B) \pm 2B\omega. \]

For \( k = 4, p = a^2 + b^2 = 4n + 1, a \equiv 1 \pmod{4} \) we obtain from (14)

\[ R_1 = \frac{\chi_3(-1)}{2} [\varphi_3(4) + i\varphi_3(4g)]. \]

We know that\(^3\) [5]

\[ \varphi_2(w^2) = -\chi_3(u)2a \]
\[ \varphi_2(2w^2) = -\chi_3(u)2b \text{ if } \chi_3(2) = -1, \lfloor b/2 \equiv 1 \pmod{4} \rfloor \]
\[ \varphi_2(\sqrt{2}w^2) = -\chi_3(u)2b \text{ if } \chi_3(2) = +1, \lfloor b/4 \equiv (-1)^{n/3} \pmod{4} \rfloor. \]

If \( \chi_3(2) = -1 \), then \( \chi_3(-1) = -1 \), and ind \( 2 \equiv 1 \) or 3 (mod 4) so that

\[ R_1 = \begin{cases} 
-(a + ib) & \text{if ind } 2 \equiv 1 \pmod{4} \\
-(a - ib) & \text{if ind } 2 \equiv 3 \pmod{4}
\end{cases} \]

or

\[ R_1 = -[a + b\chi_3(2)] \text{ if } \chi_3(2) = -1, \lfloor b/2 \equiv 1 \pmod{4} \rfloor. \quad (16) \]

\(^3\) There is a misprint in the corresponding formula (13) in [6] for \( b/4 \equiv (-1)^n \) read \( b/4 \equiv (-1)^{n/2} \). The same mistake is repeated four lines down.
If $\chi_2(2) = +1$, then $\chi_4(-1) = +1$. But $\chi_4(2) = -1$ and $\text{ind} \sqrt{2} \equiv 1$ or $3 \pmod{4}$. Hence

$$R_1 = \begin{cases} -a - bi & \text{if } \text{ind} \sqrt{2} \equiv 1 \pmod{4} \\ -a + bi & \text{if } \text{ind} \sqrt{2} \equiv 1 \pmod{4} \end{cases}$$

or

$$R_1 = -[a + b\chi_4(\sqrt{2})] \text{ if } \chi_4(2) = 1, \lfloor b/4 \equiv (-1)^{\text{ind}2} \pmod{4} \rfloor.$$ 

If $\chi_4(2) = +1$, then $\chi_4(-1) = +1$, and

$$R_1 = -a \pm bi$$

but the sign of $b$ remains undetermined.

For $k = 5$, we have by (10)

$$R_1 = \frac{1}{5} \left[ \varphi_5(4) + \alpha \varphi_5(4g) + \alpha^2 \varphi_5(4g^2) + \alpha^3 \varphi_5(4g^3) + \alpha^4 \varphi_5(4g^4) \right]$$

The $\varphi$'s have been determined previously [6] in terms of the partition

$$\{16p = x^2 + 50u^2 + 50v^2 + 125w^2 \}$$

$$\{xw = v^2 - u^2 - 4uv, x \equiv 1 \pmod{5} \}$$

to read

$$\varphi_5(4) = x - 1$$

$$\varphi_5(4g) = \frac{1}{4} \left[ -4 - x + 25w + 10(u + 2v) \right]$$

$$\varphi_5(4g^2) = \frac{1}{4} \left[ -4 - x - 25w + 10(2u - v) \right]$$

$$\varphi_5(4g^3) = \frac{1}{4} \left[ -4 - x - 25w - 10(2u - v) \right]$$

$$\varphi_5(4g^4) = \frac{1}{4} \left[ -4 - x + 25w - 10(u + 2v) \right].$$

This gives

$$R_1 = \frac{1}{4} \left[ x + \alpha(5w + 2u + 4v) + \alpha^2(-5w + 4u - 2v) \right.$$ 

$$+ \alpha^3(-5w - 4u + 2v) + \alpha^4(5w - 2u - 4v) \right].$$

In a previous paper [6] we have determined $(x, u, v, w)$ uniquely in case $\text{ind} 2 \equiv 1 \pmod{5}$ by selecting $u$ even and $v \equiv x + u \pmod{4}$. If $\text{ind} 2 \equiv m \pmod{5}$, the coefficient of $\alpha^mv$ becomes $\varphi(4g^m)$ or the coefficient of $\alpha^v$ is $\varphi(4g^m)$. This transformation is achieved if the solution:
\begin{align*}
(x, v, -u, -w) \text{ ind } 2 &\equiv 2 \pmod{5} \\
(x, u, v, w) \text{ is replaced by } (x, -v, u, -w) \text{ ind } 2 &\equiv 3 \pmod{5} \\
(x, -u, -v, w) \text{ ind } 3 &\equiv 4 \pmod{5}.
\end{align*}

As before, if \( \text{ind } 2 \equiv 0 \pmod{5} \), the indeterminancy remains.

\textbf{REFERENCES}

5. Emma Lehmer, \textit{On the number of solutions of } \( u^k + D \equiv w^2 \pmod{p} \), Pacific J. Math. \textbf{5} (1955), 103–118.
Mathematical papers intended for publication in the Pacific Journal of Mathematics should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The Pacific Journal of Mathematics is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of sustaining institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 2120 Oxford Street, Berkeley 4, California.

Printed at Kokusai Bunken Insatsuusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.
Glen Earl Baxter, An analytic problem whose solution follows from a simple algebraic identity ......................................................... 731
Leonard D. Berkovitz and Melvin Dresher, A multmove infinite game with linear payoff ................................................................. 743
Earl Robert Berkson, Sequel to a paper of A. E. Taylor ............................. 767
Gerald Berman and Robert Jerome Silverman, Embedding of algebraic systems .... 777
Peter Crawley, Lattices whose congruences form a boolean algebra .......... 787
Robert E. Edwards, Integral bases in inductive limit spaces ...................... 797
Daniel T. Finkbeiner, II, Irreducible congruence relations on lattices .......... 813
William James Firey, Isoperimetric ratios of Reuleaux polygons ............... 823
Delbert Ray Fulkerson, Zero-one matrices with zero trace ......................... 831
Leon W. Green, A sphere characterization related to Blaschke’s conjecture .... 837
Israel (Yitzchak) Nathan Herstein and Erwin Kleinfeld, Lie mappings in characteristic 2 ............................................................... 843
Charles Ray Hobby, A characteristic subgroup of a p-group .................... 853
R. K. Juberg, On the Dirichlet problem for certain higher order parabolic equations ........................................................................ 859
Melvin Katz, Infinitely repeatable games .................................................. 879
Emma Lehmer, On Jacobi functions .......................................................... 887
D. H. Lehmer, Power character matrices ................................................ 895
Henry B. Mann, A refinement of the fundamental theorem on the density of the sum of two sets of integers ........................................ 909
Marvin David Marcus and Roy Westwick, Linear maps on skew symmetric matrices: the invariance of elementary symmetric functions ........ 917
Richard Dean Mayer and Richard Scott Pierce, Boolean algebras with ordered bases ......................................................................... 925
Trevor James McMinn, On the line segments of a convex surface in $E_3$ .... 943
Frank Albert Raymond, The end point compactification of manifolds ........ 947
Edgar Reich and S. E. Warschawski, On canonical conformal maps of regions of arbitrary connectivity .............................................. 965
Marvin Rosenblum, The absolute continuity of Toeplitz’s matrices ............ 987
Lee Albert Rubel, Maximal means and Tauberian theorems ....................... 997
Helmut Heinrich Schaefer, Some spectral properties of positive linear operators .................................................................................. 1009
Jeremiah Milton Stark, Minimum problems in the theory of pseudo-conformal transformations and their application to estimation of the curvature of the invariant metric ............................................... 1021
Robert Steinberg, The simplicity of certain groups .................................... 1039
Hisahiro Tamano, On paracompactness .................................................... 1043
Angus E. Taylor, Mittag-Leffler expansions and spectral theory ................. 1049
Marion Franklin Tinsley, Permanents of cyclic matrices ............................ 1067
Charles J. Titus, A theory of normal curves and some applications ............ 1083
Charles R. B. Wright, On groups of exponent four with generators of order two .... 1097