ON JACOBI FUNCTIONS

EMMA LEHMER

The Jacobi functions[1] R_m are usually defined by

$$R_m = R_m^{(k)}(\alpha) = \sum_{s=1}^{p-2} \alpha^{\operatorname{ind} s-(m+1)\operatorname{ind}(s+1)} \tag{1}$$

where $\alpha = e^{2\pi i/k}$ and $\operatorname{ind} s = \operatorname{ind}_g s$ 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 kth power residue of p for $k = 3$, 4, 5 and 6 and for all m. The case in which 2 is a kth power residue of p still remains ambiguous.

We find it more convenient to use the character notation

$$\chi(h) = \chi_k(h) = \begin{cases} \alpha^{\operatorname{ind} h} & \text{if } (h, p) = 1 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

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

$$R_m = \sum_{s=1}^{p-2} \chi(s)[\chi(s+1)]^{-m-1} . \tag{3}$$

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

$$R_m = \chi(-1)R_{k-1-m} = \chi(-1) \sum_{s=1}^{p-2} \chi(s)\chi^m(s+1) \tag{4}$$

$$R_{k-1} = -\chi(-1) = (-1)^{n+1} . \tag{5}$$

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

LEMMA 1. *If k is odd, then*

$$R_\lambda(\alpha) = R_1(\alpha^\lambda) \text{ for } k = 2\lambda + 1 \tag{6}$$

Proof. Let $s\bar{s} \equiv 1 \pmod p$ Then

[1] Received November 17, 1959. The notation R_m is used here as in [**2**] instead of Jacobi's original ψ as in [**1**] and [**4**] to avoid conflict with Jacobsthal's ψ.

$$R_\lambda(\alpha) = \sum_{s=1}^{p-2} \chi(s)\chi^\lambda(s+1) = \sum_{s=1}^{p-2} \chi^{k-1}(\bar{s})\chi^\lambda(s+1)$$
$$= \sum_{s=1}^{p-2} \chi^\lambda(\bar{s})\chi^\lambda(\bar{s}+1) = R_1(\alpha^\lambda) .$$

LEMMA 2. *If k is even, then*

(7) $$R_\mu = \chi(4)R_1, \text{ where } k = 2\mu .$$

Proof. Using (4)

$$R_\mu = \chi(-1)\sum_{s=1}^{p-2} \chi(s)\chi^\mu(s+1) = \chi(-1)\sum_{s=1}^{p-2} \chi(s)\chi_2(s+1)$$
$$= \chi(-1)\left[\sum_{s=1}^{p-2} \chi(s)[1+\chi_2(s+1)] - \sum_{s=1}^{p-2} \chi(s)\right] .$$

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

$$R_\mu = \chi(-4)\sum_{s=1}^{p-2} \chi(s)\chi(s+1) = \chi(4)R_1 .$$

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

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

Proof.

$$R_{2\nu}^{(k)}(\alpha) = \sum_{s=1}^{p-2} \chi(s)\chi^{2\nu+1}(s+1) = \sum_{s=1}^{p-2} \chi(\bar{s})\chi^{2\nu+1}(\bar{s}+1)$$
$$= \sum_{s=1}^{p-2} \chi^{4\nu+1}(s)\chi^{2\nu+2}(\bar{s}+1) = \sum_{s=1}^{p-2} \chi^{2\nu}(s)\chi^{2\nu+1}(s+1)$$
$$= \sum_{s=1}^{p-2} \chi_{2\nu+1}^\nu(s)\chi_2(s+1)$$
$$= \sum_{s=1}^{p-2} \chi_{2\nu+1}^\nu(s)[1+\chi_2(s+1)] - \sum_{s=1}^{p-2} \chi_{2\nu+1}^\nu(s) .$$

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

$$R_{2\nu}^{(k)}(\alpha) = \sum_{t=0}^{p-2} \chi_{3\nu+1}^\nu(t^2-1) = \chi_{2\nu+1}(4)\sum_{s=1}^{p-2} \chi_{2\nu+1}^\nu(s)\chi_{2\nu+1}^\nu(s+1)$$
$$= \chi_{2\nu+1}(4)R_1^{(2\nu+1)}(\beta^\nu)$$
$$= \chi_{2\nu+1}(4)R_\nu^{(2\nu+1)}(\beta)$$

by Lemma 1.
But by (4) and Lemma 2:

$$R_{2\nu+1} = \chi(-1)R_{2\nu} = \chi_k(4)R_1 , \qquad k = 4\nu + 2 .$$

Hence by Lemma 3:

$$R_1^{(k)}(\alpha) = \chi_k(-4)R_\nu^{2\nu+1}(\beta) = \chi_k(-4)R_1^{2\nu+1}(\beta^\nu) \tag{9}$$

Armed with these relations we can express all the Jacobi functions for $k = 3, 4, 5$ and 6 in terms of the corresponding R_1 as follows.
$k = 3,\ R_2 = -1$
$k = 4,\ R_3 = -\chi(-1),\ R_2 = \chi(-1)R_1$ by (3)
$k = 5,\ R_4 = -1,\ R_3 = R_1$ by (3) and $R_2 = R_1(\alpha^2)$ by Lemma 1.
$k = 6,\ R_5 = -\chi(-1).\ \ R_4 = \chi(-1)R_1$ and $R_3 = \chi(-1)R_2$ 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's for $k = 3$ and $k = 6$.

We now proceed to expand R_1 in powers of α. If we write

$$R_1 = \chi(-1)\sum_{s=1}^{p-2}\chi(s)\chi(s+1) = \chi(-1)\sum_{\nu=0}^{k-1}a_\nu\alpha^\nu$$

then a_ν is the number of solutions of

$$s^2 + s = g^{kt+\nu} \qquad (t = 0, 1, \cdots, n-1)$$

and is given by

$$a_\nu = \sum_{\nu=0}^{k-1}\sum_{t=0}^{n-1}[1 + \chi_2(1 + 4g^{kt+\nu})] .$$

Hence

$$\begin{aligned} R_1 &= \chi(-1)\sum_{\nu=0}^{k-1}\sum_{t=0}^{n-1}\chi_2(1 + 4g^{kt+\nu})\alpha^\nu \\ &= \frac{\chi(-1)}{k}\sum_{\nu=0}^{k-1}\sum_{x=1}^{p-1}\chi_2(1 + 4x^kg^\nu)\alpha^\nu \\ &= \frac{\chi(-1)}{k}\sum_{\nu=0}^{k-1}\alpha^\nu\sum_{x=0}^{p-1}\chi_2(4g^\nu)\chi_2(x^k + (\overline{4g^\nu})) \\ &= \frac{\chi(-1)}{k}\sum_{\nu=0}^{k-1}\chi_2(4g^\nu)\psi_k(\overline{4g^\nu}) \end{aligned}$$

where [5]

$$\psi_k(D) = \sum_{x=1}^{p-1}\chi_2(x^k + D) = \begin{cases} \left(\dfrac{D}{P}\right)\psi_k(\overline{D}) & \text{if } k \text{ is even} \\[2ex] \left(\dfrac{D}{P}\right)\varphi_k(\overline{D}) & \text{if } k \text{ is odd} \end{cases}$$

and

$$\varphi_k(D) = \sum_{x=1}^{p-1} \chi_2(x)\chi_2(x^k + D) = -\left(\frac{D}{P}\right)\varphi_k(\bar{D}), \ k \text{ even}$$

is the well-known Jacobsthal [3] function. Hence

$$(10) \qquad R_1 = \begin{cases} \dfrac{\chi(-1)}{k} \displaystyle\sum_{\nu=0}^{k-1} \psi_k(4g^\nu)\alpha^\nu & \text{if } k \text{ is even} \\ \dfrac{1}{k} \displaystyle\sum_{\nu=0}^{k-1} \varphi_k(4g^\nu)\alpha^\nu & \text{if } k \text{ is odd} . \end{cases}$$

Making use of the relations [5]

$$(11) \qquad \varphi_k(m^k D) = \chi_2^{k+1}(m)\varphi_k(D)$$

$$(12) \qquad \psi_k(m^k D) = \chi_2^k(m)\psi_k(D)$$

and

$$(13) \qquad \psi_{2k}(D) = \psi_k(D) + \varphi_k(D)$$

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

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

By (11) and (12)

$$(14) \qquad R_1 = \begin{cases} \dfrac{2\chi(-1)}{k} \displaystyle\sum_{\nu=0}^{k-1} \psi_{k/2}(4g^\nu)\alpha^\nu & \text{if } k/2 \text{ is odd} \\ \dfrac{2\chi(-1)}{k} \displaystyle\sum^{k-1} \varphi_{k/2}(4g^\nu)\alpha^\nu & \text{if } k/2 \text{ is even} . \end{cases}$$

Since the functions φ and ψ have been unequivocally determined by us in [5] and [6] for $k = 3, 4, 5$ and 6 in case 2 is not a kth power residue we can apply these results directly to the determination of the corresponding R_1. For $k = 3$ let $p = A^2 + 3B^2 = 3n + 1$, $A \equiv B \equiv 1 \pmod 3$.
By (10)

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

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

$$R_1 = 2B + (B-A)\chi_3(2)\,, \qquad A \equiv B \equiv 1 \pmod 3\,. \tag{15}$$

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

$$\begin{aligned} R_1 &= \frac{1}{3}[\varphi_3(1) + \varphi_3(g)\omega + \varphi_3(g^2)\omega^2] \\ &= \frac{1}{3}[-(2A+1) + (A \pm 3B - 1)\omega + (A \mp 3B - 1)\omega^2] \\ &= -A \pm B(\omega - \omega^2) = (-A \pm B) \pm 2B\omega\,. \end{aligned}$$

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

$$R_1 = \frac{\chi_4(-1)}{2}[\varphi_2(4) + i\varphi_2(4g)]\,.$$

We know that[2] [5]

$$\begin{aligned} \varphi_2(u^2) &= -\chi_2(u)2a \\ \varphi_2(2u^2) &= -\chi_2(u)2b \text{ if } \chi_2(2) = -1,\ [b/2 \equiv 1 \bmod 4)] \\ \varphi_2(\sqrt{2}u^2) &= -\chi_2(u)2b \text{ if } \chi_2(2) = +1,\ [b/4 \equiv (-1)^{n/2} \pmod 4)]\,. \end{aligned}$$

If $\chi_2(2) = -1$, then $\chi_4(-1) = -1$, and ind $2 \equiv 1$ or $3 \pmod 4$ 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

$$R_1 = -[a + b\chi_4(2)] \text{ if } \chi_2(2) = -1,\ [b/2 \equiv 1 \pmod 4)]\,. \tag{16}$$

---

[2] 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 $\operatorname{ind}\sqrt{2} \equiv 1$ or 3 (mod 4). Hence

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

or

$$R_1 = -[a + b\chi_4(\sqrt{2})] \text{ if } \chi_2(2) = 1, [b/4 \equiv (-1)^{b/2} \pmod 4] . \tag{17}$$

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)

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

The φ's have been determined previously [6] in terms of the partition

$$\begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2 \\ xw = v^2 - u^2 - 4uv, \ x \equiv 1 \pmod 5 \end{cases}$$

to read

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

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

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

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

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

This gives

$$R_1 = \frac{1}{4}[x + \alpha(5w + 2u + 4v) + \alpha^2(-5w + 4u - 2v)$$
$$+ \alpha^3(-5w - 4u + 2v) + \alpha^4(5w - 2u - 4v)] .$$

In a previous paper [6] we have determined (x, u, v, w) uniquely in case $\operatorname{ind} 2 \equiv 1 \pmod 5$ by selecting u even and $v \equiv x + u \pmod 4$. If $\operatorname{ind} 2 \equiv m \pmod 5$, the coefficient of $\alpha^{m\nu}$ becomes $\varphi(4g^\nu)$ or the coefficient of α^ν is $\varphi(4g^{\bar{m}\nu})$. This transformation is achieved if the solution:

$$(x, u, v, w) \text{ is replaced by} \begin{cases} (x, v, -u, -w) & \operatorname{ind} 2 \equiv 2 \pmod 5 \\ (x, -v, u, -w) & \operatorname{ind} 2 \equiv 3 \pmod 5 \\ (x, -u, -v, w) & \operatorname{ind} 3 \equiv 4 \pmod 5 . \end{cases}$$

As before, if $\operatorname{ind} 2 \equiv 0 \pmod 5$, the indeterminancy remains.

References

1. P. Bachmann, *Die Lehre von der Kreistheilung* (Leipzig, 1872).
2. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem,* Amer. Math. **57** (1935), 391–424.
3. E. Jacobsthal, *Anwendungen einer Formel aus der Theorie der quadratischen Reste,* Dissertation (Berlin 1906).
4. D. H. Lehmer, *Power Character Matrices,* Pacific J. Math. **10** (1960), pp. 895–907.
5. Emma Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod p$, Pacific J. Math. **5** (1955), 103–118.
6. ———, *On Euler's criterion,* The Journ. of the Australian Math. Soc. **1** (1959), 64–70.
7. A. L. Whiteman, *The sixteenth power residue character of* 2, Canadian J. Math. **6** (1954), 364–373.