MAHLER'S MATRICES

D. H. LEHMER

(received 3 November 1959)

Recently K. Mahler [1] introduced a set of $\phi(2n)$ matrices of n rows and columns which form under multiplication the abelian group of the residue classes prime to $2n$ modulo $2n$. These remarkable matrices whose elements 0, 1 and -1, have latent roots and determinants which can be given explicitly. Thus we have new examples of matrices with given elements whose powers, roots, inverses and determinants can be written down precisely. Such matrices are often useful in testing the efficacy of methods for finding these functions for a general matrix.

The case of n odd turns out to be rather more interesting and straightforward than the even case. Although the methods used are applicable to both cases, we treat here only the odd ordered matrices. The reader will have no difficulty in modifying the argument to deal with the case of n even.

Let n be an odd integer > 1 and let m be one of the $\phi(n)$ odd integers relatively prime to n such that

$$-n < m < n. \tag{1}$$

Let $[x]$ and $\{x\}$ denote respectively the greatest integer $\leqq x$ and the fractional part of x, so that $x = [x] + \{x\}$. We denote by $A(m, n)$ the matrix whose general element is given, when $m > 0$, by

$$a_{ij} = a_{ij}(m, n) = \begin{cases} (-1)^{[(jm-i)/n]} & \text{if } n\{(jm-i)/n\} \leqq m-1 \\ 0 & \text{otherwise} \end{cases}. \tag{2}$$

For $m < 0$ we define $a_{ij}(m, n)$ by

$$a_{ij}(m, n) = a_{i,\,n+1-j}(-m, n). \tag{3}$$

Thus the matrix $A(-m, n)$ is the result of reversing the order of the rows (or columns) of $A(m, n)$.

Thus, by way of example

$$A(3, 5) = \begin{vmatrix} 1 & -1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 & 1 \\ 0 & 1 & 0 & -1 & 1 \end{vmatrix} \qquad A(-3, 5) = \begin{vmatrix} 0 & 1 & 0 & -1 & 1 \\ 0 & 1 & -1 & 0 & 1 \\ 1 & 0 & -1 & 0 & 1 \\ 1 & 0 & -1 & 1 & 0 \\ 1 & -1 & 0 & 1 & 0 \end{vmatrix}$$

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

Both matrices have roots $1, -1, i, -i$ with 1 a double root. In general, for $m > 0$, the first column of $A(m, n)$ consists of m ones followed by $n - m$ zeros. Each of the other columns is obtained from its predecessor by lowering the elements m rows. When an element would be placed below the bottom of the matrix, it is made to reappear cyclically at the top with its sign changed. For $m < 0$ the first column consists of $n + m$ zeros followed by $|m|$ ones and the elements of the succeeding columns are lifted instead of lowered. In particular $A(1, n)$ is the unit matrix I, while $A(-1, n)$ has its ones on the sinister diagonal.

If k is any number prime to n there is exactly one odd representative m, satisfying (1), such that

$$k \equiv m \pmod{n}.$$

For uniformity we define $A(k, n)$ to be $A(m, n)$. With this understanding, Mahler's result may be stated

$$A(k, n)A(h, n) = A(hk, n). \tag{4}$$

For example the matrices $A(3, 5)$ and $A(-3, 5)$ are mutually inverse since $3(-3) \equiv 1 \pmod{5}$.

The following numerical functions will be used in what follows.

$\phi(r)$ the totient function of Euler
$\mu(r)$ the function of Möbius, $\mu(x) = 0$ if x is not an integer.
$\sigma_k(r)$ the sum of the k-th powers of the divisors of r
$\nu(r)$ $= \sigma_0(r)$; the number of divisors of r
$\varepsilon(x)$ $= \begin{cases} 1 \text{ if } x \text{ is an integer} \\ 0 \text{ otherwise} \end{cases}$
$c_r(k)$ the sum of the k-th powers of the primitive r-th roots of unity sometimes called Ramanujan's sum.
$Q_r(x)$ the irreducible polynomial whose roots are the primitive r-th roots of unity, $Q_r(x) = x^{\phi(r)} + \cdots$.
(m/n) Jacobi's symbol
$\Delta(r)$ the greatest common divisor of n and $m^r - 1$.

We denote by $e = e(m, n)$ the exponent of m modulo n, that is the least positive h for which

$$m^h \equiv 1 \pmod{n}.$$

In view of (4),

$$[A(m, n)]^e = I.$$

Thus we have at once the theorems

THEOREM 1. *The latent roots of $A(m, n)$ are e-th roots of unity.*

THEOREM 2. *The determinant of $A(m, n)$ is ± 1 and is a real character modulo n.*

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

We now prove

THEOREM 3. *The trace of* $A(m, n)$ *is* $\Delta(1)$.

PROOF. For brevity we write Δ for $\Delta(1)$. Suppose first that $m > 0$. Let $m - 1 = \Delta s$, $n = \Delta t$.

By (2) with $i = j$

$$a_{ii} = \begin{cases} (-1)^{[is/t]} & \text{if } t\{is/t\} \leqq s \\ 0 & \text{otherwise} \end{cases}.$$

Hence the trace T of $A(m, n)$ is

$$T = \sum_{i=1}^{n} a_{ii} = \sum_{t\{is/t\} \leqq s} (-1)^{[is/t]}.$$

Now since m and n are both odd, t is odd and s is even and prime to t. Hence

$$[is/t] \equiv t[is/t] = is - t\{is/t\} \equiv t\{is/t\} \pmod 2.$$

Furthermore $t\{is/t\}$ is a periodic function of i of period t which, because s and t are relatively prime, ranges over the numbers $r = 0(1)t - 1$ without repetitions or omissions for $i = 1(1)t$. Hence we can write

$$T = \Delta \sum_{i=1}^{t} (-1)^{t\{is/t\}} = \Delta \sum_{r \leqq s} (-1)^r = \Delta.$$

We consider now the case $m < 0$. Setting

$$|m| + 1 = \Delta s, \qquad n = \Delta t$$

in (3) and (2) we find

$$a_{ii}(m, n) = a_{i, n+1-i}(|m|, n) = \begin{cases} (-1)^{[(i\Delta s - n - 1)/n]} & \text{if } n\{(i\Delta s - 1)/n\} \leqq \Delta s - 2 \\ 0 & \text{otherwise} \end{cases}.$$

Now

$$[(i\Delta s - n - 1)/n] \equiv 1 + n\{i\Delta s - 1)/n\} + i\Delta s - 1 \equiv n\{(i\Delta s - 1)/n\} \pmod 2.$$

This last function is periodic in i of period t and so

$$T = \sum_{i=1}^{n} a_{ii} = \Delta \sum_{i=1}^{t} (-1)^{n\{(i\Delta s - 1)/n\}} = \Delta S$$

$$n\{(i\Delta s - 1)/n\} \leqq \Delta s - 2.$$

It remains to show that the sum $S = 1$. Actually the conditions under the summation operator does not permit i to become t, for if $i = t$

$$n\{(i\Delta s - 1)/n\} = n - 1 \geqq |m| + 1 = \Delta s.$$

But if $i = 1(1)t - 1$ the numbers u_i such that

$$is \equiv u_i \pmod t \qquad (0 < u_i < t)$$

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

range over the same set in some order. Now

$$n\{i\Delta s - 1)/n\} = \Delta u_i - 1$$

and so

$$S = \sum_{\Delta u-1 \leqq \Delta s-2} (-1)^{\Delta u-1}$$

If $\Delta > 1$

$$S = -\sum_{u=1}^{s-1} (-1)^u = 1.$$

If $\Delta = 1$

$$S = \sum_{\nu=0}^{s-2} (-1)^\nu = 1.$$

This completes the proof of Theorem 3.

By Theorem 1 the roots $A(m, n)$ are among the primitive d-th roots of unity where d ranges over the divisors of e. Hence we can write the characteristic polynomial of $A(m, n)$ as a product or irreducible polynomials as follows:

$$|A(m, n) - \lambda I| = -\prod_{d|e} [Q_d(\lambda)]^{M(d)} \tag{5}$$

where $M(d) \geqq 0$ denotes the multiplicity of the primitive d-th roots of unity. Hence to give a complete account of the roots of $A(m, n)$ we have only to find $M(d)$ as a function of d, m, and n. To begin with, we have

THEOREM 4. *The $\nu(e)$ multiplicities $M(d)$ satisfy the $\nu(e)$ linear equations*

$$\sum_{\delta|e} M(\delta)\, c_\delta(d) = \Delta(d), \quad (d|e). \tag{6}$$

PROOF. Let d be a fixed divisor of e. Consider the trace T_d of the matrix $[A(m, n)]^d$. Since, by (4),

$$[A(m, n)]^d = A(m^d, n),$$

Theorem 3 with m^d replacing m, tells us that

$$T_d = \Delta(d).$$

On the other hand, T_d is simply the sum of the d-th powers of all the roots of $A(m, n)$. That is,

$$T_d = \sum_{\delta|e} M(\delta)\, c_\delta(d).$$

Hence Theorem 4 is proved.

We proceed now to solve the system (6) for the unknown values $M(d)$. For this purpose we prepare a lemma giving an important orthogonal property of Ramanujan's sum $c_r(k)$.

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

LEMMA 1. *Let k and t be any divisors of a positive integer e.*

Then

$$S_e(k,t) = \sum_{\delta \mid e} c_t(e/\delta)\, c_\delta(k) = \begin{cases} e & \text{if } kt = e \\ 0 & \text{otherwise} \end{cases}.$$

PROOF. We may use the known facts [2]

$$\sum_{r=1}^{\infty} c_t(r) r^{-s} = \zeta(s) \sum_{\delta \mid t} \mu(t/\delta)\, \delta^{1-s} \tag{7}$$

$$\sum_{r=1}^{\infty} c_r(k) r^{-s} = \sigma_{1-s}(k)/\zeta(s). \tag{8}$$

It is evident that $S_e(k,t)$ is the coefficient of e^{-s} in the product of (7) and (8). That is

$$\sum_{e=1}^{\infty} S_e(k,t)\, e^{-s} = \Big(\sum_{\delta \mid t} \mu(t/\delta)\, \delta^{1-s}\Big)\, \sigma_{1-s}(k)$$

$$= \Big(\sum_{r=1}^{\infty} r\mu(t/r) r^{-s}\Big)\Big(\sum_{r=1}^{\infty} r\varepsilon(k/r) r^{-s}\Big).$$

Identifying the coefficients of e^{-s} on both sides we obtain

$$S_e(k,t) = \sum_{\delta \mid e} \delta\mu(t/\delta)\,(e/\delta)\,\varepsilon(k\delta/e)$$

$$= e \sum_{\delta \mid t} \mu(t/\delta)\,\varepsilon(k\delta/e).$$

Here we have replaced the condition $\delta \mid e$ by $\delta \mid t$ since otherwise $\mu(t/\delta)$ is zero. Setting $kt/e = x$ and replacing δ by t/δ we have

$$S_e(k,t) = e \sum_{\delta \mid t} \mu(\delta)\,\varepsilon(x/\delta).$$

If x is not an integer then $\varepsilon(x/\delta)$ vanishes and so $S_e(k,t) = 0$. If x is an integer the non-zero terms correspond to $\delta \mid x$. But $x \mid t$ since $t = ex/k$ and $k \mid e$. Hence

$$S_e(k,t) = e \sum_{\delta \mid x} \mu(\delta) = \begin{cases} e & \text{if } x = 1 \\ 0 & \text{if } x > 1 \end{cases}.$$

But $x = 1$ is equivalent to $kt = e$. This completes the proof of the lemma.

THEOREM 5. *For each divisor d_1 of e*

$$eM(d_1) = \sum_{\delta \mid e} c_{e/\delta}(e/d_1)\, \Delta(\delta). \tag{9}$$

PROOF. If we multiply both members of (6) by $c_{e/d}(e/d_1)$ and the sum over all divisors d of e we obtain

$$\sum_{d \mid e} \sum_{\delta \mid e} M(\delta)\, c_\delta(d)\, c_{e/d}(e/d_1) = \sum_{d \mid e} c_{e/d}(e/d_1)\, \Delta(d). \tag{10}$$

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

The left member may be written, replacing d by e/d

$$\sum_{\delta \mid e} M(\delta) \sum_{d \mid e} c_d(e/d_1)\, c_\delta(e/d).$$

Applying the lemma with $k = e/d_1$ and $t = \delta$ the inner sum vanishes except when $\delta e/d_1 = e$, that is when $\delta = d_1$. Hence the left member of (10) reduces simply to $eM(d_1)$, which is the theorem. We have thus given an explicit determination of the function $M(d)$. With this we may substitute into (5) to obtain the characteristic polynomial of $A(m, n)$ decomposed into its irreducible factors. However, a simpler description of this polynomial free from the rather complicated function [3]

$$c_r(k) = \frac{\mu\left(\dfrac{r}{(k, r)}\right)}{\phi\left(\dfrac{r}{(k, r)}\right)} \phi(r)$$

is afforded by our next theorem. In preparation we need the following simple lemma.

LEMMA 2. *Let k, r be any positive integers and define*

$$S_k(r) = \sum_{\delta \mid r} c_k(\delta)\, \mu(r/\delta).$$

Then

$$S_k(r) = r\mu(k/r).$$

PROOF. Recalling the fact that

$$\sum_{t=1}^{\infty} \mu(t)\, t^{-s} = 1/\zeta(s)$$

we see from (7) that

$$\begin{aligned}
\sum_{r=1}^{\infty} S_k(r)\, r^{-s} &= \sum_{r=1}^{\infty} \sum_{\delta \mid r} c_k(\delta)\, \mu(r/\delta)\, (r/\delta)^{-s} \delta^{-s} \\
&= \Big(\sum_{t=1}^{\infty} \mu(t)\, t^{-s}\Big)\Big(\sum_{\delta=1}^{\infty} c_k(\delta) \delta^{-s}\Big) \\
&= \sum_{\delta \mid k} \mu(k/\delta)\, \delta^{1-s} \\
&= \sum_{r=1}^{\infty} r\mu(k/r)\, r^{-s}.
\end{aligned}$$

Comparing coefficients of r^{-s} on both sides gives the lemma.

THEOREM 6. *The characteristic polynomial of $A(m, n)$ is given by*

$$|A(m, n) - \lambda I| = -\prod_{\delta \mid e} (\lambda^\delta - 1)^{E(\delta)}$$

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

where

$$dE(d) = \sum_{\delta \mid d} \Delta(\delta)\, \mu(d/\delta). \tag{11}$$

PROOF. It is well-known that

$$Q_d(\lambda) = \prod_{\delta \mid d} (\lambda^\delta - 1)^{\mu(d/\delta)}. \tag{12}$$

Hence by (5)

$$|A(m, n) - \lambda I| = - \prod_{d \mid e} (\lambda^d - 1)^{E(d)}$$

where, in view of (12) and (9)

$$\begin{aligned} eE(d) &= \sum_{\delta \mid e/d} eM(d\delta)\, \mu(\delta) \\ &= \sum_{\delta \mid e/d} \mu(\delta) \sum_{\delta_1 \mid e} c_{e/\delta_1}\left(\frac{e}{d\delta}\right) \Delta(\delta_1) \\ &= \sum_{\delta_1 \mid e} \Delta(\delta_1) \sum_{\delta \mid e/d} c_{e/\delta_1}(\delta)\, \mu\left(\frac{e}{d\delta}\right). \end{aligned}$$

By Lemma 2, the inner sum is

$$S_{e/\delta_1}(e/d) = \frac{e}{d}\, \mu(d/\delta_1).$$

Substitution gives

$$dE(d) = \sum_{\delta_1 \mid e} \Delta(\delta_1)\, \mu(d/\delta_1).$$

But $\mu(d/\delta_1)$ vanishes unless $\delta_1 | d$. This gives us (11).

THEOREM 7.

$$\sum_{\delta \mid e} \delta E(\delta) = \sum_{\delta \mid e} \phi(\delta)\, M(\delta) = n.$$

PROOF. The degree of the characteristic polynomial of $A(m, n)$ is n. More generally we have

THEOREM 8. *If* $d|e$, $\sum_{\delta \mid d} \delta E(\delta) = \Delta(d)$.

This follows from Möbius inversions of (11). Of course

$$\Delta(e) = n$$

to agree with Theorem 7. Incidentally, by Theorem 7, $M(1)$ and $M(2)$ are of opposite parity.

THEOREM 9.

$$\sum_{\delta \mid e} E(\delta)\, \varepsilon(\delta/d) = M(d). \tag{13}$$

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

PROOF. The factor $(x^\delta - 1)^{E(\delta)}$ contains $E(\delta)$ roots $\exp 2\pi i/d$ or no such root according as $d|\delta$ or not. Hence this factor's contribution to the total multiplicity of the primitive d-th roots of unity is precisely the left member of (13).

Theorem 9 affords an easy way of determining the function $M(d)$ and is generally to be preferred to (9).

THEOREM 10. *The determinant* $|A(m, n)| = -(-1)^{M(1)}$.

PROOF. Put $\lambda = 0$ in Theorem 6. Then $|A(m, n)| = -(-1)^{\Sigma}$ where $\Sigma = \Sigma_{\delta|e} E(\delta)$.

By Theorem 9 with $d = 1$, $\Sigma = M(1)$.

For our final theorem we need

LEMMA 3. *Let* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ *be the canonical factorization of* n *into powers of distinct primes. Let* g_i *be chosen so that*

$$g_i \equiv \begin{cases} \text{a primitive root of } p_i^{\alpha_i} \pmod{p_i^{\alpha_i}} \\ 1 \pmod{n/p_i^{\alpha_i}}. \end{cases}$$

Then every totative m *of* n *has an unique representation*

$$m \equiv g_1^{\beta_1} g_2^{\beta_2} \cdots g_t^{\beta_t} \pmod{n} \begin{Bmatrix} \beta_i = 0(1)\phi(p_i^{\alpha_i}) - 1 \\ i = 1(1)t \end{Bmatrix}.$$

PROOF. The $\phi(n)$ numbers

$$g_1^{\beta_1} g_2^{\beta_2} \cdots g_t^{\beta_t}$$

are clearly prime to n. We have to show that no two are congruent (mod n). If two were congruent their ratio would produce a representation of unity in the form

$$g_1^{\gamma_1} g_2^{\gamma_2} \cdots g_t^{\gamma_t} \equiv 1 \pmod{n} \qquad (|\gamma_i| < \phi(p^{\alpha_i}))$$

with some $\gamma_\nu \neq 0$. This would imply

$$g_\nu^{\gamma_\nu} \equiv 1 \pmod{p_\nu^{\alpha_\nu}}.$$

But g_ν is a primitive root of p_ν. Hence $\gamma_\nu = 0$, a contradiction.

THEOREM 11. *The determinant of* $A(m, n)$ *is Jacobi's symbol* (m/n).

PROOF. Let p be any prime factor of n so that

$$n = p^\alpha n_0 \qquad (p \nmid n_0)$$

and let g be a primitive root of p^α. Consider first the case in which

$$m \equiv \begin{cases} g \pmod{p^\alpha} \\ 1 \pmod{n_0}. \end{cases}$$

The exponent e of m (mod n) is clearly

$$e = \phi(p^\alpha) = p^{\alpha-1}(p - 1).$$

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

Let δ be any divisor of e. We proceed to calculate $\Delta(\delta)$ in the three possible cases:

Case I: $(p-1) \nmid \delta$. In this case $m^\delta - 1$ is not divisible by p but is divisible by n_0.
Hence

$$\Delta(\delta) = n_0.$$

Case II: $\delta = p^{\beta-1}(p-1)$, $(1 \leqq \beta < \alpha)$. In this case $m^\delta - 1$ is divisible by p^β but not by $p^{\beta+1}$.
Hence

$$\Delta(\delta) = p^\beta n_0.$$

Case III: $\delta = e$. In this case

$$\Delta(\delta) = \Delta(e) = n = p^\alpha n_0.$$

We can now determine $E(d)$ for every divisor d of e by (11).

If $d = 1$, (11) gives

$$E(1) = \Delta(1) = n_0.$$

If $d > 1$ but not divisible by $p-1$ we have, from (11) and Case I,

$$dE(d) = \sum_{\delta \mid d} \Delta(\delta)\mu(d/\delta) = n_0 \sum_{\delta \mid d} \mu(d/\delta) = 0.$$

Hence

$$E(d) = 0 \quad \text{if } (p-1) \nmid d.$$

Now we take the case of $d = p-1$. Then (11) gives

$$\begin{aligned}(p-1)E(p-1) &= \sum_{\delta \mid p-1} \Delta(\delta)\mu((p-1)/\delta) \\ &= n_0 \sum_{\delta \mid p-1} \mu\left(\frac{p-1}{\delta}\right) + (p-1)n_0 = (p-1)n_0\end{aligned}$$

by Case I and Case II.
Hence

$$E(p-1) = n_0.$$

If $\alpha > 1$ we proceed to consider the cases (if any) of

$$d = (p-1)p^{\beta-1} \qquad (1 < \beta < \alpha).$$

Then

$$\begin{aligned}dE(d) &= \sum_{h \mid p-1} \sum_{k=1}^{\beta} \Delta(hp^{k-1})\mu(p^{\beta-k}(p-1)/h) \\ &= \sum_{h \mid p-1} \mu\left(\frac{p-1}{h}\right)(\Delta(hp^{\beta-1}) - \Delta(hp^{\beta-2})).\end{aligned}$$

By Case I this difference of Δ's vanishes unless $h = p-1$.

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

Hence by Case II

$$dE(d) = \Delta((p-1)p^{\beta-1}) - \Delta((p-1)p^{\beta-2})$$
$$= n_0 p^{\beta} - n_0 p^{\beta-1} = n_0 d.$$

Therefore

$$E(d) = n_0.$$

Finally let $d = e = (p-1)p^{\alpha-1}$. Here we have as before

$$eE(e) = \sum_{\delta \mid e} \Delta(\delta)\mu(e/\delta) = \Delta(e) - \Delta(e/p) = n_0 p^{\alpha} - n_0 p^{\alpha-1}.$$

Hence

$$E(e) = n_0.$$

Thus all the non-zero values of $E(d)$ are n_0. They correspond to $d = 1$ and $d = (p-1)p^{\beta}$ $(0 \leqq \beta \leqq \alpha - 1)$. We now compute

$$M(1) = \sum_{d \mid e} E(d) = n_0(1 + \sum_{\beta=0}^{\alpha-1} 1) = (\alpha+1)n_0.$$

By Theorem 10, the determinant of $A(m, n)$ in this case is $(-1)^{\alpha}$.

We now apply Lemma 3 to complete the proof of the theorem for a general m. Given any m prime to $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ we may replace m by the congruent number modulo n

$$g_1^{\beta_1} g_2^{\beta_2} \cdots g_t^{\beta_t}$$

referred to in Lemma 3. By (4)

$$A(m, n) = \prod_{i=1}^{t} A(g_i^{\beta_i}, n) = \prod_{i=1}^{t} (A(g_i, n))^{\beta_i}.$$

Applying the above reasoning to each $A(g_i, n)$ we find for the determinant of $A(m, n)$

$$|A(m, n)| = \prod_{i=1}^{t} (-1)^{\alpha_i \beta_i} = \left(\frac{g_1^{\beta_1} \cdots g_t^{\beta_t}}{p_1^{\alpha_1} \cdots p_t^{\alpha_t}}\right) = \left(\frac{m}{n}\right).$$

This proves Theorem 11.

We note that, by (4) above we can infer that the set of $\phi(n)$ determinants $|A(m, n)|$ constitute a real "character" modulo n. Which of the 2^t different real characters modulo n is $|A(n, m)|$ is the question answered by Theorem 11.

It follows from Theorem 11 that there is reciprocity between the determinants of $A(m, n)$ and $A(m, n)$ namely

$$|A(m, n)| = |A(n, m)|(-1)^{(n-1)(m-1)/4}.$$

In conclusion we illustrate Theorems 6—9 by the example of $n = 385 = 5 \cdot 7 \cdot 11$ and $m = 3$. Here we find $e = 60$ and tabulate the pertinent functions as follows:

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press

δ	$3^\delta \pmod{385}$	$\Delta(\delta)$	$\delta E(\delta)$	$E(\delta)$	$M(\delta)$	$\phi(\delta) M(\delta)$
1	3	1	1	1	15	15
2	9	1	0	0	12	12
3	27	1	0	0	9	18
4	81	5	4	1	9	18
5	243	11	10	2	10	40
6	344	7	6	1	9	18
10	144	11	0	0	8	32
12	141	35	24	2	6	24
15	342	11	0	0	6	48
20	331	55	40	2	6	48
30	309	77	60	2	6	48
60	1	385	240	4	4	64
			385			385

Hence the characteristic polynomial of $A(3, 385)$ is

$$|A(3, 385) - \lambda I|$$
$$= -(\lambda-1)(\lambda^4-1)(\lambda^5-1)^2(\lambda^6-1)(\lambda^{12}-1)^2(\lambda^{20}-1)^2(\lambda^{30}-1)^2(\lambda^{60}-1)^4$$
$$= -Q_1^{15} Q_2^{12} Q_3^9 Q_4^9 Q_5^{10} Q_6^9 Q_{10}^8 Q_{12}^6 Q_{15}^6 Q_{20}^6 Q_{30}^6 Q_{60}^4.$$

To illustrate Theorem 10 and 11 we note that $M(1)$ is odd and

$$\left(\frac{3}{385}\right) = \left(\frac{3}{5}\right)\left(\frac{3}{7}\right)\left(\frac{3}{11}\right) = (-1)(-1)(+1) = +1.$$

By Theorem 5,

$$eM(1) = \sum_{\delta \mid e} c_\delta(e)\, \Delta(e/\delta) = \sum_{\delta \mid e} \phi(\delta)\, \Delta(e/\delta).$$

Hence we have the rather curious fact that (m/n) is $+1$ or -1 according as the integer

$$e^{-1} \sum_{\delta \mid e} \phi(\delta)\, \Delta(e/\delta)$$

is odd or even.

Bibliography

[1] Mahler, K., A Matrix Representation of the Primitive Residue Classes Modulo $2n$, Proc Amer. Math. Soc. 8 (1957), 525–531.

[2] Titchmarsh, E. C., The Theory of the Riemann Zeta-function, Oxford (1951), p. 10.

[3] Vandiver H. S. and Nicol C. A. suggest that this statement be known as the Dedekind-Hölder theorem. [see Proc. Nat. Acad. Sci. U.S.A. 44 (1958), 917–918].

The University of California, Berkeley.

https://doi.org/10.1017/S1446788700026215 Published online by Cambridge University Press