CYCLOTOMY AND TRINOMIAL CONGRUENCES*

BY

L. E. DICKSON

1. **Introduction.** In the algebraic theory of cyclotomy we regard as known (or computed by tables of indices) one† or more of the functions $R(1, n)$, which Jacobi denoted by ψ_n. By rational operations and root extractions we obtain Jacobi's function F, then the periods, and finally the e^2 cyclotomic constants (k, h); see §6.

We here develop an arithmetical theory valid for every prime $p=ef+1$. The $R(1, n)$ are not computed by tables of indices, but are found in the simpler cases by representations of multiples of p by binary quadratic forms, and in general by a system of Diophantine equations (§§13–17). The cyclotomic constants (k, h) are found from linear equations, some of which are derived from linear relations between pairs of the functions $R(m, n)$. In an earlier memoir‡ we treated in full the cases $e=3, 4, 5, 6, 8, 10, 12$. Here we treat the cases in which e is a prime or a double of a prime. In particular, we find the number of solutions of $x^e+y^e\equiv\pm 1 \pmod p$.

2. **Notations, results assumed.** For proofs, see D.

Let g be a primitive root of a prime $p>2$. Let e be a divisor of $p-1=ef$. Let R be any root $\neq 1$ of $x^p=1$. The *periods* are

$$\eta_k = \sum_{t=0}^{f-1} R^{g^{et+k}} \qquad (k = 0, 1, \cdots, e-1). \tag{1}$$

Let (k, h) denote the number of sets of values of t and z, each chosen from $0, 1, \cdots, f-1$, for which

$$1 + g^{et+k} \equiv g^{ez+h} \pmod p. \tag{2}$$

$$\eta_m\eta_{m+k} = \sum_{h=0}^{e-1} (k, h)\eta_{m+h} + fn_k, \quad n_0 = 1 \ (f \text{ even}), \quad n_{e/2} = 1 \ (f \text{ odd}), \tag{3}$$

while the remaining n_k are zero.

$$\begin{gathered}(e-k, h-k) = (k, h), \\ (k, h) = (h, k) \ (f \text{ even}), \quad (k, h) = (h+\tfrac{1}{2}e, k+\tfrac{1}{2}e) \ (f \text{ odd});\end{gathered} \tag{4}$$

* Presented to the Society, December 28, 1934; received by the editors December 31, 1934.

† One function suffices when e is a prime <83, but not for $e=83$ or 107. See Kronecker, Journal für Mathematik, vol. 93 (1882), pp. 338–64; K. Schwering, ibid., vol. 102 (1888), p. 56, and Acta Mathematica, vol. 11 (1887–88), p. 119.

‡ American Journal of Mathematics, vol. 57 (1935), in press, cited as D.

$$\sum_{h=0}^{e-1}(k, h) = f - n_k \qquad (k = 0, 1, \cdots, e-1). \tag{5}$$

Let α be any $(p-1)$th root $\neq 1$ of unity. With Jacobi, write

$$F(\alpha) = \sum_{k=0}^{p-2} \alpha^k R^{g^k}. \tag{6}$$

In particular, let $\alpha = \beta^m$, where β is a primitive eth root of unity. Then

$$F(\beta^m) = \sum_{j=0}^{e-1} \beta^{mi}\eta_j, \qquad F(\beta^n)F(\beta^{-n}) = (-1)^{nf}p, \tag{7}$$

if n is not divisible by e. Since $R^{p-1} + \cdots + R + 1 = 0$ is irreducible* in the field of the rational functions with integral coefficients of a primitive kth root of unity when k is not divisible by p, it follows that $F(\alpha) \neq 0$.

If no one of m, n, $m+n$ is divisible by e,

$$R(m, n, \beta) \equiv \frac{F(\beta^m)F(\beta^n)}{F(\beta^{m+n})} = \sum_{k=0}^{e-1} \beta^{nk} \sum_{h=0}^{e-1} \beta^{-(m+n)h}(k, h), \tag{8}$$

$$R(n, m) = R(m, n) = (-1)^{nf}R(-m-n, n), \tag{9}$$

$$R(m, n)R(-m, -n) = p. \tag{10}$$

$$R(m, n, \beta^j) = R(jm, jn, \beta). \tag{11}$$

$$R(2r, 2s, \beta)_e = R(r, s, \beta^2)_E, \text{ if } e = 2E; \tag{12}$$

$$(k, h)_E = (k, h) + (k+E, h) + (k, E+h) + (E-k, h-k). \tag{13}$$

$$F(-1)F(\alpha^2) = \alpha^{2m}F(\alpha)F(-\alpha), \quad g^m \equiv 2 \pmod{p}. \tag{14}$$

When g is replaced by a new primitive root g^r of p,

$$R(m, n) \text{ becomes } R(mr', nr'), \ r'r \equiv 1 \pmod{e}. \tag{15}$$

3. **Relations between the coefficients of $R(1, n)$.** We employ (9) for $m = 1$ and then (8) for $m = -1-n$. The product of the two powers of β now has the exponent $nk+h$. Eliminate h by use of $nk+h \equiv i \pmod{e}$. We get

$$(-1)^{nf}R(1, n) = \sum_{i=0}^{e-1} B(i, n)\beta^i, \qquad B(i, n) = \sum_{k=0}^{e-1}(k, i-nk). \tag{16}$$

When n and k are fixed, $i-nk$ ranges with i over a complete set of residues modulo e. Hence by (5),

$$\sum_{k,i}(k, i-nk) = \sum_{k,h}(k, h) = \sum_{k}(f - n_k) = ef - 1,$$

* Kronecker, Journal de Mathématiques, vol. 19 (1854), pp. 177–92.

since a single n_k is 1 and the others are 0. Hence

$$\sum_{i=0}^{e-1} B(i, n) = p - 2. \tag{17}$$

THEOREM* 1. *If e is prime† to 6,*

$$\sum_{i=0}^{e-1} iB(i, n) \equiv 0, \qquad \sum_{i=0}^{e-1} i^2 B(i, n) \equiv 0 \pmod{e}. \tag{18}$$

Since $p = ef+1 > 2$, f is even. Write $B(i)$ for $B(i, n)$. By (4),

$$(0, r),\ (r, 0),\ (-r, -r),\ r \not\equiv 0 \pmod{e}, \tag{19}$$

are equal. They are respectively terms of $B(r)$ with $k=0$, $B(n, r)$ with $k=r$, $B(-r, -nr)$ with $k=-r$. Since the sum of the three arguments of B is zero, the sum of the corresponding terms of (18_1) is zero.

Next let $r \not\equiv 0$, $s \not\equiv 0$, $r \not\equiv s \pmod{e}$. Then each of

$$(r, s) = (-r, s-r) = (-s, r-s) = (s, r) = (s-r, -r) = (r-s, -s) \tag{20}$$

has incongruent arguments each $\not\equiv 0 \pmod{e}$; while no two have congruent first arguments and congruent second arguments. Hence these (r, s) coincide in sets of six. They are terms of

$$B(s + nr),\ B(s - r - nr),\ B(r - s - ns),\ B(r + ns),$$
$$B(-r + ns - nr),\ B(-s + nr - ns),$$

the sum of whose arguments is zero. This proves (18_1).

In (18_2), the sum of the coefficients of the three numbers (19) and the sum of the coefficients of the six numbers (20) are respectively

$$(1 + n + n^2)r^2,\ 2(1 + n + n^2)(r^2 - rs + s^2).$$

Multiply (5) by k^2 and sum for k. Thus

$$\sum_{k,h=0}^{e-1} k^2(k, h) = fN, \qquad N = \sum_{k=1}^{e-1} k^2 = \tfrac{1}{6}e(e-1)(2e-1).$$

Since $e \equiv \pm 1 \pmod 6$, N is a multiple of e. In the double sum the sum of the coefficients of the three numbers (19) or six numbers (20) is respectively

$$0 + r^2 + r^2,\ r^2 + r^2 + s^2 + s^2 + 2(s-r)^2 = 4(r^2 - rs + s^2).$$

---

* The case in which $n=1$ and e is a prime >3 is due to K. Schwering, Journal für Mathematik, vol. 93 (1882), pp. 334–37. His formulas have $-2rs$ in error for $-rs$. By (17) and Theorem 1, $1+R(1, n)$ is divisible by $(1-\beta)^3$. Our new application of Theorem 1 is given in §13.

† When e is composite (16) is not to be reduced to degree $<e-1$ by the equation satisfied by β.

THEOREM 2. *If e is prime to 2, 3 and 5,*

$$\sum_{i=0}^{e-1} i^4 B(i, n) \equiv 0 \pmod{e}.$$

The sum of the coefficients of the three numbers (19) and the sum of the coefficients of the six numbers (20) are respectively

$$2r^4J, \qquad 2\{r^4 + s^4 + (r - s)^4\}J, \qquad J = 1 + 2n + 3n^2 + 2n^3 + n^4.$$

But $2r^4$ and $2\{r^4+s^4+(r-s)^4\}$ are evidently the corresponding sums in

$$\sum_{k,h=0}^{e-1} k^4(k, h) = fM, \qquad M = \sum_{k=1}^{e-1} k^4 = (e - 1)e(2e - 1)(3e^2 - 3e - 1)/30.$$

The final factor is a multiple of 5 if $e \equiv -1$ or $2 \pmod 5$. Also, $2e-1 \equiv 0$ if $e \equiv -2 \pmod 5$. Hence M is a multiple of e if e is prime to 5 and 6.

Since $1+\beta+\cdots+\beta^{e-1}=0$, we may eliminate the constant term from (16) and obtain (for e prime to 6)

$$R(1, n, \beta) = \sum_{i=1}^{e-1} a_i\beta^i, \qquad a_i = B(i, n) - B(0, n), \tag{21}$$

$$\sum_{i=1}^{e-1} a_i = p - 2 - e\sum_{k=0}^{e-1} (k, -nk) \equiv -1 \pmod{e}, \tag{22}$$

$$\sum_{i=1}^{e-1} ia_i \equiv 0, \qquad \sum_{i=1}^{e-1} i^2a_i \equiv 0, \qquad \sum_{i=1}^{e-1} i^4a_i \equiv 0 \pmod{e}, \tag{23}$$

where e is prime to 30 for the third. Every linear homogeneous function of the a_i which is a multiple of e for all consistent values of the (k, h) is a linear combination of the three in (23), at least when e is a prime.

Write $e=2E+1$. In the terms $i=E+1, \cdots, 2E$ write $I=e-i$. Then the last two of (23) give

$$\sum_{i=1}^{E} i^2b_i \equiv 0, \qquad \sum_{i=1}^{E} i^4b_i \equiv 0 \pmod{e}, \qquad b_i = a_i + a_{e-i}, \tag{24}$$

when e is prime to 3 or 15, respectively.

4. **To express p as a sum of multiples of squares.** By (10), (11), and (21),

$$p = R(1, n, \beta)R(1, n, \beta^{-1}) = \sum a_i^2 + \sum_{i=1}^{e-2} (\beta^i + \beta^{-i}) \sum_{j=1}^{e-1-i} a_ja_{j+i}.$$

In the terms with $i \geqq E+1$, write $i=e-I$. Hence if $e=2E+1$,

$$p - \sum_{i=1}^{e-1} a_i^2 = \sum_{i=1}^{E} (\beta^i + \beta^{-i})C_i, \qquad C_i = \sum_{j=1}^{e-1-i} a_ja_{j+i} + \sum_{j=1}^{i-1} a_ja_{j+e-i}, \tag{25}$$

where the final sum is absent if $i=1$.

Let e be an odd prime. Then $\beta^{e-1}+\cdots+\beta+1$ is irreducible in the field of rational numbers. Thus $C_1, \cdots, C_E$ are equal, and

$$p = \sum_{i=1}^{e-1} a_i^2 - C/E, \qquad C = \sum_{i=1}^{E} C_i = \sum a_1 a_2, \tag{26}$$

where the final sum is a symmetric function. Next

$$(e-1)^2\left\{\sum_{i=1}^{e-1} a_i^2 - E^{-1}\sum a_1 a_2\right\} - \left(\sum_{i=1}^{e-1} a_i\right)^2 = eM, \tag{27}$$

$$M = (e-2)\sum_{i=1}^{e-1} a_i^2 - 2\sum a_1 a_2, \qquad D = \sum_{i=1}^{E} (a_i - a_{e-i})^2, \tag{28}$$

$$M - ED = \Delta = (E-1)\sum_{i=1}^{E} b_i^2 - 2\sum b_1 b_2, \tag{29}$$

where the final sum is symmetric in $b_1, \cdots, b_E$ defined in (24). The proof of (29) follows from

$$2\sum b_1 b_2 = \sum b_i b_j = \sum (a_i a_j + a_{e-i}a_{e-j} + 2a_i a_{e-j}), \quad i \neq j.$$

THEOREM 3. $(e-1)^2 p = (\sum a_i)^2 + e(ED+\Delta)$.

Case $e=5$. Then $\Delta = (b_1-b_2)^2$. By (24), $b_1 - b_2 = 5W$, where W is an integer. Hence

$$16p = (\sum a_i)^2 + 125W^2 + 10(a_1 - a_4)^2 + 10(a_2 - a_3)^2. \tag{30}$$

Denote (29) by Δ_E and consider the like function Δ_j of $b_1, \cdots, b_j$. Define

$$L_{j-1} = (j-1)b_j - \sum_{i=1}^{j-1} b_i. \tag{31}$$

The recursion formula

$$(j-1)\Delta_j = j\Delta_{j-1} + L_{j-1}^2, \quad \Delta_1 = 0, \tag{32}$$

yields Δ_j as a linear combination of $L_{j-1}^2, \cdots, L_1^2$:

$$\Delta_2 = L_1^2, \quad 2\Delta_3 = L_2^2 + 3L_1^2, \quad 3\Delta_4 = L_3^2 + 2L_2^2 + 6L_1^2,$$
$$12\Delta_5 = 3L_4^2 + 5L_3^2 + 10L_2^2 + 30L_1^2, \quad 10\Delta_6 = 2L_5^2 + 12\Delta_5.$$

Case $e=7$. Then (24) give $b_1 \equiv b_2 \equiv b_3 \pmod 7$. Thus

$$L_1 = b_2 - b_1 = 7v, \quad L_2 = 2b_3 - b_1 - b_2 = 7W,$$
$$72p = 2(\sum a_i)^2 + 42D + 7^3(W^2 + 3v^2), \tag{33}$$
$$D = (a_1 - a_6)^2 + (a_2 - a_5)^2 + (a_3 - a_4)^2.$$

Case $e=11$. Then

$$1200p = 12(\sum a_i)^2 + 660D + 11(3L_4^2 + 5L_3^2 + 10L_2^2 + 30L_1^2). \tag{34}$$

By (24),

$$b_4 \equiv -2b_1 + 4b_2 - b_3, \qquad b_5 \equiv 3b_1 + 3b_2 - 5b_3 \pmod{11}, \tag{35}$$

$$L_3 + 2L_2 + 2L_1 \equiv 0, \quad L_4 - L_2 + 3L_1 \equiv 0 \pmod{11}. \tag{36}$$

But it is not possible to segregate from Δ_5 a square divisible by 11, unlike the cases $e=5$, $e=7$.

5. **Sets of conjugate** $R(1, j)$. If j is prime to e and if β is replaced by β^j, the coefficients a_i in (21) are permuted cyclically, whence $\sum a_i$ is unaltered. For example, if $e=5$ and $j=3$, the substitution is $(a_1\ a_2\ a_4\ a_3)$. By (11), $R(m, n)$ becomes $R(jm, jn)$, which will be called a *conjugate* to $R(m, n)$. Hence each $R(m, n)$ is conjugate to some $R(1, -)$.

Let $e=2E+1$ be a prime >3. By (9), $R(1, 1)$ equals $R(1, e-2)$, which is conjugate to $R(E, 1)=R(1, E)$ since $E(e-2)\equiv 1 \pmod{e}$.

Consider a new $R(1, n)$, where $2\leqq n\leqq e-3$, $n\neq E$. It equals $R(1, e-1-n)$, which is conjugate to $R(m, 1)=R(1, e-1-m)$ if $m(1+n)\equiv -1 \pmod{e}$. Again, $R(1, n)$ equals $R(n, e-1-n)$, which is conjugate to $R(1, e-1-t)=R(1, t)$ if $tn\equiv 1 \pmod{e}$. We now have six $R(1, -)$ whose second arguments are congruent modulo e to

$$n,\ 1/n,\ -1-n,\ -1-1/n,\ -1/(n+1),\ -n/(n+1).$$

These form a group (of cross ratios). Hence they are distinct unless

$$n^2 + n + 1 \equiv 0, \quad (2n+1)^2 \equiv -3 \pmod{e}, \qquad e \equiv 1 \pmod{3}. \tag{37}$$

THEOREM 4. *If e is a prime >3, $R(1, 1), \cdots, R(1, e-2)$ fall into complete sets of conjugates as follows: when $e=6r+5$, one set of three, and r sets of six; when $e=6r+1$, one set of three, $r-1$ sets of six, and the set*

$$R(1, n),\ R(1, e-1-n),\ n^2+n+1\equiv 0 \pmod{e}. \tag{38}$$

6. **Determination of the** e^2 **cyclotomic constants** (k, h) **when** e **is a prime** >3. For $n\leqq e-2$, let $R(1, n)$ be unaltered when β is replaced by β^j, $1<j<e$. By (11), $R(1, n)=R(j, jn)$. By (9), one of j, jn must be congruent modulo e to 1 or n. If $jn\equiv 1$, either $j=n$, or $-1-j\equiv n$ and $n^2+n+1\equiv 0$. Next, let $j=n$. If $n^2\equiv 1$, then $n\equiv 1$, $j\equiv 1$, contrary to hypothesis. Hence $-n-n^2\equiv 1 \pmod{e}$. Hence $R(1, n)$ is unaltered if, and only if, $j=n$, $n^2+n+1\equiv 0 \pmod{e}$. Then $e\equiv 1 \pmod 6$ by (37). Since $n^3\equiv 1 \pmod{e}$, the substitution which replaces β by β^n is of period 3. Hence for (38) there are only $\frac{1}{3}(e-1)$ distinct a_i in R, while any R except those two has $e-1$ distinct a_i.

The linear relations (5) with $k \geqq \frac{1}{2}(e+1)$ reduce by (4) to those with $k \leqq \frac{1}{2}(e-1)$, whence there are only $\frac{1}{2}(e+1)$ independent relations. Then Theorem 4 shows that the sum of all the a's in the $R(1, n)$, one from each set of conjugates, increased by the preceding $\frac{1}{2}(e+1)$, is $\frac{1}{6}(e+1)(e+2)$ whether $e \equiv 5$ or 1 (mod 6). But this is the number of reduced (i, j) which remain after deleting duplicates by (4). In proof, we retain $(0, 0)$ and $(0, r)$ for $r = 1, \cdots, e-1$. Each of the latter is one of a set of three equal (i, j) by (19). The remaining $e^2-3(e-1)-1$ fall into sets of six by (20). Hence the number of reduced (i, j) is

$$1 + e - 1 + \tfrac{1}{6}(e^2 - 3e + 2) = \tfrac{1}{6}(e + 1)(e + 2).$$

These $\frac{1}{6}(e+1)(e+2)$ linear equations in the same number of unknowns are linearly independent and hence determine the unknowns uniquely, and therefore determine all the cyclotomic constants. First, we note that (8) and (7_2) imply

$$[F(\beta)]^e = pR(1, 1)R(1, 2) \cdots R(1, e - 2). \tag{39}$$

Hence the $R(1, n)$ and their conjugates determine the $F(\beta^m)$, $m = 0, \cdots, e-1$. By (7_1), the latter determine the periods η_j. Then (3) determine $(k, 0)$, $(k, 1), \cdots, (k, e-1)$ for $k = 0, \cdots, e-1$, since the determinant of their coefficients is the cyclic determinant having $\eta_0, \cdots, \eta_{e-1}$ in the first row and hence is the product of the linear functions (7_1) whose values are the $F(\beta^m)$. But the latter were proved in §2 to be not zero.

THEOREM 5. *Let e be a prime >3. The e^2 numbers (i, j) reduce to $M = \frac{1}{6}(e+1) \cdot (e+2)$ after deleting duplicates by* (4). *These M reduced (i, j) are uniquely determined by M linear equations composed of* (5) *for $k = 0, \cdots, \frac{1}{2}(e-1)$, and $M - \frac{1}{2}(e+1)$ equations expressing the a_{in} in terms of the (k, h), where there are $\frac{1}{3}(e_1-1)$ distinct a_{in} in case* (38), *and $e-1$ a_{in} for the further $R(1, n)$ in Theorem* 4, *one from each set of conjugates.*

For example, if $e = 5$, $M = 7$, $M - \frac{1}{2}(e+1) = 4$, and we employ only the four a_{i1}.

We shall give details only for $(0, 0)$. By D, §10, either of

$$x^e + y^e \equiv \pm 1 \pmod{p = ef + 1}, \ f \text{ even}, \tag{40}$$

has exactly $2e+e^2$ $(0, 0)$ solutions.

7. **To find $(0, 0)$.** Employ a second subscript n in (22). Then

$$\sum_{n=1}^{e-2} \sum_{i=1}^{e-1} a_{in} = (e - 2)(p - 2) - e(e - 2)(0, 0) - eS, \quad S = \sum_{k=1}^{e-1} \sum_{n=1}^{e-2} (k, -nk).$$

Let e be an odd prime. Each k is not divisible by e. For a fixed k, and $n=1, \cdots, e-2$, the residues modulo e of $-nk$ are $1, \cdots, e-1$, except k. Hence

$$S = \sum_{k=1}^{e-1}\Big\{\sum_{h=1}^{e-1}(k,h) - (k,k)\Big\}.$$

We may extend the summation from $h=0$ by subtracting the new term $(k, 0)$. But $(k, k)=(-k, 0)$ and $-k$ ranges with k over $1, \cdots, e-1$ modulo e. Thus

$$S = \sum_{k=1}^{e-1}\sum_{h=0}^{e-1}(k,h) - 2\sum_{h=1}^{e-1}(0,h) = (e-1)f - 2\{f-1-(0,0)\}$$

by (5). From eS eliminate $ef=p-1$. Hence

$$\sum_{n=1}^{e-2}\sum_{i=1}^{e-1} a_{in} = p - 3e + 1 - e^2(0,0). \tag{41}$$

This determines (0, 0). The left member may be simplified by Theorem 4. If $e=5$ we obtain, in accord with (66) of D,

$$25(0,0) = p - 14 - 3\sum_{i=1}^{4} a_{i1}; \tag{42}$$

$$3\sum_{1}^{6} a_{i1} + 2\sum_{1}^{6} a_{i2} = p - 20 - 49(0,0) \text{ if } e = 7. \tag{43}$$

In Theorem 3, $D\geqq 0, \Delta\geqq 0$, and p is not a square. Hence

$$(e-1)p^{1/2} > \sum_{i=1}^{e-1} a_{in}. \tag{44}$$

This with (41) gives*

$$e^2(0,0) > p - 3e + 1 - (e-1)(e-2)p^{1/2}. \tag{45}$$

Cyclotomy for $e=2E$, E an odd prime, §§8–12

8. Sets of conjugate $R(i, j)$. If m and n are both even,

$$R(2m, 2n) = R(e - 2m - 2n, 2n),$$

and the latter first argument is double an odd integer. Hence we may assume that m is odd and prime to E. Thus $mx\equiv 1 \pmod{E}$ determines x, and $R(2m, 2n)$ is conjugate to $R(2, 2nx)$. The latter is found by (12). The dis-

* The writer gave a different proof in Journal für Mathematik, vol. 135 (1909), pp. 181–88. At bottom of p. 188, insert $p\neq 41$.

tribution of the $R(2, \text{even})$ into conjugate sets is therefore obtained from Theorem 4 applied to E in place of e, with subsequent multiplication of arguments by 2.

Consider therefore $R(m, n)$, where m is odd. If $m \neq E$, $mx \equiv 1 \pmod{e}$ is solvable for x. Next, $R(E, k)$ is excluded if k is a multiple of E. If k is even, pass to the equal $R(-E-k, k)$, whose first argument is odd and prime to e. Hence any R is conjugate to an $R(1, -)$. We extend the definition of conjugate so that $(-1)^f R$ is conjugate to R.

THEOREM 6. *If $\frac{1}{2}e = E$ is an odd prime, $R(1, 1), \cdots, R(1, e-2)$ fall into $\frac{1}{2}(E+1)$ sets of conjugates as follows:*

$$R(1, 1) = (-1)^f R(1, e-2);$$

$$R(1, E) = (-1)^f R(1, E-1);$$

$$R(1, j) = (-1)^f R(1, e-1-j), \quad R(1, x) = (-1)^f R(1, e-1-x),$$

$$1 < j < E, \quad j \text{ odd}, \quad xj \equiv 1 \pmod{e}.$$

9. To find $(0, 0)$ and $(0, E)$. We have

$$\beta^E = -1, \quad \beta^{E-1} - \cdots - \beta + 1 = 0,$$

$$R(1, n) = \sum_{i=0}^{E-1} r_i \beta^i = \sum_{i=1}^{E-1} R_i \beta^i, \quad R_i = r_i - (-1)^i r_0,$$

$$\sum_{i=1}^{E-1} (-1)^i R_i = \sigma - E r_0, \quad \sigma = \sum_{i=0}^{E-1} (-1)^i r_i = R(1, n) \text{ for } \beta = -1,$$

$$R(1, n) = \sum_{k=0}^{e-1} \beta^{nk} Y(k, \beta), \quad Y(k, \beta) = \sum_{h=0}^{e-1} \beta^{-(1+n)k} (k, h),$$

by (8). Henceforth, let n be odd.* Then by (5)

$$Y(k, -1) = \sum_{h=0}^{e-1} (k, h) = f - n_k, \quad \sigma = \sum_{k=0}^{e-1} (-1)^k (f - n_k) = -\sum_{k=0}^{e-1} (-1)^k n_k,$$

whence $\sigma = -(-1)^f$. We get r_0 from (16) by using the terms with $i = 0$ and $i = E$.

THEOREM 7. *If $\frac{1}{2}e = E$ and n are odd,*

$$R(1, n) = \sum_{i=1}^{E-1} R_i \beta^i, \quad \rho(1, n) \equiv \sum_{i=1}^{E-1} (-1)^i R_i = -(-1)^f \{1 + E r(1, n)\},$$

$$r(1, n) = \sum_{k=0}^{e-1} \{(k, -nk) - (k, E - nk)\}.$$

* If n were even, pass to $R(1, -1-n)$ by (9).

If $\frac{1}{2}e=E$ is an odd prime, we find that

$$\rho(1,1)+2\sum\rho(1,n)=-(-1)^f\{E+E^2(0,0)-E^2(0,E)\}, \tag{46}$$

where $\rho(1,1)$ and the $\rho(1,n)$ together correspond to the $R(1,k)$ with odd k's such that a single one is chosen from each set of conjugates in Theorem 6. For example, the $k>1$ are

3 if $e=6$; 5, 7 if $e=10$; 3, 7, 9 if $e=14$; 3, 5, 7, 11, 13 if $e=22$.

Special cases of (13) are

$$(0,0)_E=(0,0)+3(0,E),\ f \text{ even};\quad (0,0)_E=3(0,0)+(0,E),\ f \text{ odd}. \tag{47}$$

By this and (46) we get $(0,0)$ and $(0,E)$ in terms of the $\rho(1,k)$. To find the latter we shall next evaluate the $R(1,k)$.

10. **Determination of the $R(1,k)$.** By (14) for $\alpha=\beta^j$,

$$\begin{aligned} F(\beta^E)F(\beta^{2j})&=\beta^{2mj}F(\beta^j)F(\beta^{j+E}),\\ R(E,2j)&=\beta^{2mj}R(j,j+E). \end{aligned} \tag{48}$$

Multiply the former by $F(\beta^j)/(F(\beta^{j+E})F(\beta^{2j}))$. Thus

$$R(j,E)=\beta^{2mj}R(j,j),\quad R(1,E)=\beta^{2m}R(1,1). \tag{49}$$

By (48) for $j=\frac{1}{2}(E-1)$ and (9),

$$R(1,E-1)=(-1)^{f(E-1)/2}\beta^{m(E-1)}R(1,\tfrac{1}{2}(E-1)). \tag{50}$$

By (49_2) and (9),

$$R(1,E-1)=(-1)^f\beta^{2m}R(1,1),\quad F(\beta^2)F(\beta^{E-1})=(-1)^f\beta^{2m}F(\beta)F(\beta^E), \tag{51}$$

$$R(2,E-1)=(-1)^f\beta^{2m}R(1,E)=(-1)^f\beta^{4m}R(1,1), \tag{52}$$

by (49). By (50) and (51_1),

$$R(1,\tfrac{1}{2}(E-1))=(-1)^{f(E+1)/2}\beta^{m(3-E)}R(1,1). \tag{53}$$

By (12), $R(2,2)=R(1,1)_E$ is known. Replacing β by $\beta^{(E-1)/2}$, we get $R(E-1,E-1)=R(2.E-1)$. Then by (52), (53), (51), (49_2), we get $R(1,1)$, $R(1,\frac{1}{2}(E-1))$, $R(1,E-1)$, $R(1,E)$.

If $e=6$, we have the desired $R(1,1)$, $R(1,3)$. If $e=10$, we have the desired $R(1,1)$, $R(1,5)$, $R(1,7)$. By (8),

$$R(m,t)R(n,m+t)=R(m,n)R(m+n,t). \tag{54}$$

For $E>3$, take $m=n=1$, $t=(E-3)/2$. Thus

$$R(1,\tfrac{1}{2}(E-3))R(1,\tfrac{1}{2}(E-1))=R(1,1)R(2,\tfrac{1}{2}(E-3)). \tag{55}$$

By (53) this gives

(56) $R(1, 2) = \beta^{4m}R(2, 2)$ if $e = 14$; $R(1, 4) = \beta^{8m}R(2, 4)$ if $e = 22$.

For $e=14$, replace β by β^9 in $R(1, 11)=(-1)^fR(1, 2)$; we get $R(1, 9)$. Hence we have the desired $R(1, 1)$, $R(1, 3)$, $R(1, 7)$, $R(1, 9)$.

For $e=22$, replace β by β^{13} in $R(1, 17)=(-1)^fR(1, 4)$; we get $R(1, 13)$. We have also $R(1, 1)$, $R(1, 5)$, $R(1, 11)$. We desire also $R(1, 3)$ and $R(1, 7)$. By (54) for $m=1, t=2, n=5$,

(57) $$R(1, 2)R(5, 3) = R(1, 5)R(6, 2), \quad R(3, 5) = R(1, 5, \beta^5),$$

which give $R(1, 2)$. Replacing β by β^7 in $R(1, 19)=(-1)^fR(1, 2)$, we get $R(1, 7)$. By (54) for $m=n=1, t=2$,

(58) $$R(1, 2)R(1, 3) = R(1, 1)R(2, 2),$$

which gives $R(1, 3)$. But $R(1, 7)$ and $R(1, 3)$ were not found linearly. Neither is a product of a unit by any R not conjugate to itself.

11. **Theory*** for $e=14$. We have

(59) $$\beta^7 = -1, \quad \beta^6 - \beta^5 + \beta^4 - \beta^3 + \beta^2 - \beta + 1 = 0.$$

Thus $B=\beta^2$ is a primitive seventh root of unity. We may regard as known (§14) the a_i in

(60) $$R(1, 1)_{E=7} = a_1B + \cdots + a_6B^6.$$

Replacing B by B^3 (and reducing by $B^7=1$), we get $R(3, 3)$ for $E=7$. We now write β^2 for B, reduce by (59_1), and by (12) get

$$R(4, 4) = -a_2\beta + a_4\beta^2 - a_6\beta^3 + a_1\beta^4 - a_3\beta^5 + a_5\beta^6,$$
$$R(2, 6) = R(6, 6) = -a_6\beta + a_5\beta^2 - a_4\beta^3 + a_3\beta^4 - a_2\beta^5 + a_1\beta^6.$$

By (52), (53), (49_1) and the remark below (56),

(61) $$R(1, 1) = (-1)^f\beta^{-4m}R(2, 6), \quad R(1, 3) = (-1)^f\beta^{-8m}R(2, 6),$$
$$R(1, 7) = (-1)^f\beta^{-2m}R(2, 6), \quad R(1, 9) = (-1)^f\beta^{8m}R(4, 4).$$

By (46)

(62) $$\rho(1, 1) + 2\rho(1, 3) + 2\rho(1, 7) + 2\rho(1, 9) = -(-1)^f\{7 + 49(0, 0) - 49(0, 7)\}.$$

By Theorem 7, $\rho(1, n)$ is derived at once from $R(1, n)$.

I. Let $m\equiv 0 \pmod 7$, i.e., 2 is a residue of a seventh power modulo p. For $p<1000$ this case occurs only when $p=631, 673, 953$. Then

$$\rho(1, j) = (-1)^f\sum_1^6 a_i \text{ if } j = 1, 3, 7 \text{ or } 9.$$

* Details for $e=6$ and $e=10$ were given in D.

Cancelling $7(-1)^f$ from (62), we get

$$-1-7(0,0)+7(0,7)=\sum a_i. \tag{63}$$

This with (47) yields at once (0, 0) and (0, 7).

II. $m\equiv 4 \pmod 7$; true for $p<1000$ only when $p=29, 43, 127, 421, 701, 967$. We get

$$\rho(1,j)=(-1)^f\{\sum a_i-7a_k\},$$

$$k=5 \text{ if } j=1,\ k=3 \text{ if } j=3,\ k=6 \text{ if } j=7 \text{ or } 9;$$

$$7(0,0)-7(0,7)=-1-a_1-a_2+a_3-a_4+3a_6. \tag{64}$$

III. $m\equiv 2 \pmod 7$. Thus $p=71, 281, 449, 547, 659, 743, 911$, etc. Now $k=6$ if $j=1$, $k=5$ if $j=3$, $k=3$ if $j=7$ or 9,

$$7(0,0)-7(0,7)=-1-a_1-a_2+3a_3-a_4+a_5. \tag{65}$$

This and the further cases are similar to II. For, if we use a new primitive root G, where $g\equiv G^t \pmod p$, m is replaced by $M\equiv mt \pmod{p-1}$. We can choose t so that $M\equiv 0$ or $4 \pmod 7$.

12. **Determination of all (k, h).** Let $e=2E$, E a prime >3. There remain $m=(e+1)(e+2)/6$ reduced (i, j) after deleting duplicates by (4). There are $M=(E+1)(E+2)/6$ reduced $(k, h)_E$, which we regard as known by the theory for E. To these correspond M linear equations (13); the first terms (k, h) of their second members may be eliminated from the $E+1$ independent relations (5) for $k=0, 1, \cdots, E$. We must evidently get the $\frac{1}{2}(E+1)$ independent relations (5) with $0\leqq k\leqq\frac{1}{2}(E-1)$ involving the $(k, h)_E$. We discard these relations between knowns, and retain only the $\frac{1}{2}(E+1)$ new relations.

By Theorem 6 the $R(1, n)$ form $\frac{1}{2}(E+1)$ sets of conjugates. Each $R(1, n)$ is a linear combination of $\beta, \cdots, \beta^{E-1}$. Retaining only one R from each set, we have $\frac{1}{2}(E+1)(E-1)$ coefficients. We now have

$$M+\tfrac{1}{2}(E+1)+\tfrac{1}{2}(E+1)(E-1)=m$$

linear equations for the m reduced (i, j). These equations are independent by the discussion following (39).

Diophantine equations in the a_j, §§13–17

13. **General theory.** Let e be an odd prime. With the abbreviation (25) for the quadratic functions C_i of the a_j, we have the system of $E=\frac{1}{2}(e-1)$ quadratic Diophantine equations

$$C_1=C_2=\cdots=C_E, \qquad p=\sum_{j=1}^{e-1} a_j^2-C_1 \tag{66}$$

in the $e-1$ unknowns a_i. This system was seen to be equivalent to

$$(67) \qquad p = R(1, n, \beta)R(1, n, \beta^{-1}), \qquad R(1, n, \beta) = \sum_{i=1}^{e-1} a_i\beta^i.$$

But* p is a product of $e-1$ prime ideals (each of norm p). When $e<23$, each ideal is a principal ideal, since there is a single class of ideals for the field F of rational functions of the primitive eth root β of unity. Hence $p=up_1 \cdots p_{e-1}$, where u is a unit of F and p_j is a polynomial in β^j with integral coefficients independent of j. Let $f(\beta)$ be a product† of $\frac{1}{2}(e-1)$ of the p_j such that $f(\beta^{-1})$ is the product of the remaining p's. Since $p_1 \cdots p_{e-1}$ is a symmetric function with integral coefficients of the roots of $\beta^{e-1}+\cdots+\beta+1=0$, it is an integer I. By $p=uI$, $u=\pm 1$. Thus $\pm p=f(\beta)f(\beta^{-1})$. The lower sign is excluded by §4. Thus $u=1$ and

$$p = vf(\beta)\cdot v^{-1}f(\beta^{-1}), \quad v = v(\beta), \quad v^{-1} = v(\beta^{-1}).$$

The unit v is the product‡ of an integral power of β by a polynomial $P(\beta+\beta^{-1})$. Hence $P^2=1$ and $v=\pm\beta^k$. Thus

$$(68) \qquad p = \pm F(\beta)\cdot \pm F(\beta^{-1}), \qquad F(\beta) = \beta^k f(\beta) = \sum_{j=1}^{e-1} a_j\beta^j.$$

Write $\beta F=\sum A_i\beta^i$, summed for $i=1, \cdots, e-1$. Then

$$(69) \qquad A_1 = -a_{e-1}, \quad A_{i+1} = a_i - a_{e-1} \qquad (i = 1, \cdots, e-2),$$

$$(70) \qquad \sum A_j \equiv \sum a_j, \quad \sum jA_j \equiv \sum ja_j + \sum a_j \pmod e,$$

where j takes the values $1, \cdots, e-1$. Hence if $\beta^n F=\sum N_i\beta^i$,

$$(71) \qquad \sum N_j \equiv \sum a_j, \quad \sum jN_j \equiv \sum ja_j + n\sum a_j \pmod e.$$

But $\sum a_j \not\equiv 0 \pmod e$ by Theorem 3 or (17). Hence in (68) there is a single value of β^k for which $\sum ja_j \equiv 0 \pmod e$, and hence, by (23), such that (68) is a decomposition (67) available for cyclotomy.

When β is replaced by its powers in turn, the a_i undergo the substitutions of a cyclic group of order $e-1$. These substitutions leave unaltered (23_1), and the system (23).

THEOREM 8. *If $e=5$, the eight solutions of* (66) *for which $\sum ja_j \equiv 0 \pmod 5$ are all derived from one by the powers of $(a_1a_2a_4a_3)$ and changing all signs.*

---

* Kummer. See Hilbert's report, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4 (1894), p. 328.

† When $e=5$, $f(\beta)$ is p_1p_2, p_3p_4, p_1p_3 or p_2p_4.

‡ Kummer. See Hilbert's report, p. 336.

14. **Case** $e=7$. The only factorizations $p=f(\beta)f(\beta^{-1})$ are

$$p_1p_2p_3\cdot p_6p_5p_4,\quad p_1p_3p_5\cdot p_6p_4p_2,\quad p_1p_4p_5\cdot p_6p_3p_2, \tag{72}$$

$$p_1p_2p_4\cdot p_6p_5p_3. \tag{73}$$

Since (73) is unaltered when β is replaced by β^2, it corresponds to (67) with $n=2$. This is true by §15 or directly by

$$\begin{aligned} R(1,2) &= r+s(\beta+\beta^2+\beta^4)+t(\beta^3+\beta^5+\beta^6), \\ r &= (0,0)+3(1,3)+3(1,5), \\ s &= (0,1)+(0,2)+(0,4)+(1,2)+(1,4)+(1,5)+(2,4), \\ t &= (0,3)+(0,5)+(0,6)+(1,2)+(1,3)+(1,4)+(2,4), \end{aligned} \tag{74}$$

$$4p=(s+t-2r)^2+7(s-t)^2. \tag{75}$$

The replacement of β by β^3 induces $S=(a_1a_5a_4a_6a_2a_3)$. The same replacement carries (72_1) to (72_3) and the latter to (72_2).

THEOREM 9. *If* $e=7$, *all solutions of* (66) *having* $\sum ja_j\equiv 0 \pmod 7$ *are of two types. For one type, the six* a_j *are equal in sets of three and correspond to* $R(1,2)$. *The twelve solutions of the other type correspond to* $R(1,1)$ *and are all derived from one by the powers of* S *and changing all signs.*

By (5) and (74), we find that (43) is equivalent to

$$3\sum_1^6 a_{i1}-14r=-p-16-49(0,0), \qquad R(1,1)=\sum_1^6 a_{i1}\beta^i, \tag{76}$$

since $3(s+t)=p-2-r$. Hence the first square in the decomposition (75) determines r apart from sign. The sign is fixed by the fact that (76) must yield an integer for $(0,0)$. This is simpler than using

$$R(1,2)=R(1,1)R(1,1,\beta^2)/R(1,1,\beta^3). \tag{77}$$

15. Kummer* proved that, if e is a prime,

$$R(1,n,\beta)\doteq\pm\beta^s\prod p(\beta^{m_h}), \tag{78}$$

where the product extends over the $\frac{1}{2}(e-1)$ positive integers $h<e$ such that $h+[nh]>e$. Here $[x]$ denotes the least positive residue of x, and $hm_h\equiv 1 \pmod e$. Also $p(\alpha)$ is a prime ideal factor of p, and may be replaced by a polynomial in α if $e<23$.

For brevity write m for $p(\beta^m)$. Replacing β by β^{-1}, we get $e-m$.

16. **Case** $e=11$. By (78), $R(1,1)$ and $R(1,2)$ are the products of units $\pm\beta^j$ by the products of

* Journal für Mathematik, vol. 35 (1847), pp. 361–63; Journal de Mathématiques, vol. 12 (1847), pp. 185–212, where he gave a $p(\alpha)$ for $e=5, 7, 11, 13, 17, 19$, for all primes $p<1000$, $p\equiv 1 \pmod e$.

(79) $$2\ 5\ 7\ 8\ 10, \qquad 3\ 5\ 7\ 9\ 10,$$

respectively. Replacing β by β^{-1} (i.e., subtracting each symbol from 11) in (79_1), we get the complementary set 9 6 4 3 1; the symbols in the two sets are together $1, \cdots, 10$ rearranged. In all there are 16 pairs of complementary sets. We list the sets containing 1.

I. 1 2 3 4 5	VI. 1 2 4 6 8	XI. 1 3 5 7 9
II. 1 2 3 4 6	VII. 1 2 5 7 8	XII. 1 3 6 7 9
III. 1 2 3 5 7	VIII. 1 2 6 7 8	XIII. 1 4 5 8 9
IV. 1 2 3 6 7	IX. 1 3 4 5 9	XIV. 1 4 6 8 9
V. 1 2 4 5 8	X. 1 3 4 6 9	XV. 1 5 7 8 9
		XVI. 1 6 7 8 9

Let I denote also the pair of complementary sets containing I. Likewise for II, etc. The replacement of β by β^2 permutes the pairs as follows:

(80) (I, XI, XIII, X, VIII) (II, VI, V, XII, IV) (III, XV, XIV, VII, XVI),

while the sets of the pair IX are interchanged. This replacement of β by β^2 induces the substitution

(81) $$s = (a_1a_6a_3a_7a_9a_{10}a_5a_8a_4a_2)$$

on the coefficients of $a_1\beta + \cdots + a_{10}\beta^{10}$. Hence all solutions of (66) are obtained by applying powers of s to the solutions obtained from I, II, III, IX. We seek properties of solutions a_i which will discard the last two cases and hence retain only solutions from I and II, or if we prefer, X and VI, which occur in the cycles of (80) having I and II. Note that X and VI are complementary to (79) and hence correspond to $R(1, 1)$ and $R(1, 2)$.

The set IX is unaltered by $(\beta\beta^3\beta^9\beta^5\beta^4)$, whence the resulting ten a_i are equal in sets of five. Such immediately detected solutions of (66) yield neither $R(1, 1)$ nor $R(1, 2)$.

By (54) with $m=n=1, t=14$, and (9), (11), we get

(82) $$R(1, 1, \beta) = R(1, 2, \beta^6)R(1, 2, \beta^7)/R(1, 2, \beta^3),$$

which is quickly verified by (8). The denominator is equal to $p/R(1, 2, \beta^8)$. Theoretically we could use (82) to show that the solution a_i obtained from III yields neither $R(1, 2)$ nor $R(1, 1)$. Practically it is simpler to verify that we do not then obtain an integral value for (0, 0) by

(83) $$3\sum a_{i1} + 6\sum a_{i2} = p - 32 - 121(0, 0),$$

to which (41) reduces when $e=11$ by Theorem 4.

We employ the $p(\alpha)$ in Kummer's table cited in the last foot-note. We

choose n to make the final sum in (71) a multiple of $e=11$. Then the new $\sum ja_j \equiv 0 \pmod{11}$. Finally we change all signs (if necessary) to make $\sum a_i \equiv -1$ as in (22).

$$p = 683, \quad p(\beta) = 2 + \beta$$

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	$\sum a_i$
$-\beta^6$ I	12	12	16	16	22	−6	10	14	6	7	109
$-\beta^2$ II	2	−24	−6	−6	−10	−10	−1	−12	−4	4	−67
$-\beta^5$ III	−11	−6	2	−2	−24	−14	−8	−14	0	−12	−89

Then (83) holds modulo 121 if and only if

$$(\sum a_{i1}, \sum a_{i2}) = (109, -67) \text{ or } (-89, -89).$$

The second case is excluded since the two products (79) are distinct. Hence the first and second rows of our tablette give the coefficients of $R(1, 1)$ and $K(1, 2)$ respectively.* Also, $(0, 0) = 6$.

$$p = 991, \quad p(\beta) = 2 + \beta + \beta^3$$

$-\beta^7$ I	8	8	4	29	10	18	6	18	26	4	$\sum = 131$
$-\beta^6$ II	−6	−14	18	−10	−13	−16	−12	−8	−4	−2	$\sum = -67$
$-\beta^4$ III	10	4	−10	−12	4	−4	−19	2	−18	−2	$\sum = -45$

Here (83) holds only when the first row gives $R(1, 1)$ and the second $R(1, 2)$. Thus $(0, 0) = 8$.

$$p = 199, \quad p(\beta) = 1 + \beta - \beta^2$$

$-\beta^4$ I	2	2	−4	4	6	8	4	−5	6	−2	$\sum = 21$
$-\beta^5$ II	2	−2	−8	−10	4	−6	0	0	−2	−1	$\sum = -23$
$-\beta^7$ III	6	6	7	8	16	2	2	6	4	8	$\sum = 65$

The first row gives $R(1, 1)$, the second $R(1, 2)$, the third is excluded by (83).

$p = 23$, $p(\beta) = 1 + \beta + \beta^9$. Then $-\beta^5$ I, β^9 II, $-\beta^6$ III have $\sum a_i = 21, -12, -1$. Here (83) holds only when the sums are 21 and -12 or both -1, the last contrary to (79).

We have treated the four p's < 1000 for which $p(\beta)$ has fewer than four terms.

17. **Case** $e = 13$. By (78), $R(1, 1)$, $R(1, 2)$ and $R(1, 3)$ are the products of units $\pm\beta^s$ by the products of

* Apart from a power of (81), depending on the root β chosen. Likewise for the similar later statements.

(84) $\qquad 2, 3, 4, 5, 6, 12;\ 3, 4, 6, 8, 11, 12;\ 2, 4, 5, 6, 10, 12,$

respectively. Since $R(1, 3)$ is unaltered when β is replaced by β^3, its 12 coefficients a_i are equal in sets of three. No other factorization of p has this property.

The replacement of β by β^2 gives rise to a cyclic substitution S on the twelve powers of β. Applying S, S^3, S to the sets complementary (§16) to (84), we get

(85) $\qquad A = 1, 2, 3, 5, 7, 9;\ B = 1, 2, 3, 4, 7, 8;\ C = 1, 2, 3, 5, 6, 9.$

There are exactly 32 decompositions of p into two complementary products of six factors. Of them, (84_3) and C are permuted by S. The others form five cycles of six, those of a cycle being permuted by S. It suffices to know one entry from each cycle. We may take them to be A, B and

(86) $\qquad D = 1, 2, 3, 4, 5, 6;\ E = 1, 2, 3, 4, 5, 7;\ F = 1, 3, 4, 5, 6, 11.$

The choice $A, \cdots, F$ facilitates forming and checking the products. Each product of six is multiplied by a unit $\pm\beta^s$ uniquely determined (§13) by

$$\sum a_j \equiv -1, \qquad \sum j a_j \equiv 0 \pmod{13}.$$

Theoretically it would be possible to prove by means of

$$(87)\quad R(1, 1) = \frac{R(1, 2, \beta^4)R(1, 2, \beta^7)}{R(1, 2, \beta^2)}, \qquad R(1, 3) = \frac{R(1, 2, \beta^7)R(1, 2, \beta^8)}{R(1, 2, \beta^2)}$$

that $R(1, 1)$, $R(1, 2)$, $R(1, 3)$ correspond to A, B, C, respectively, while (86) are excluded. Practically we make use of

$$(88)\qquad 3\sum a_{i1} + 6\sum a_{i2} + 2\sum a_{i3} = p - 38 - 169(0, 0),$$

to which (41) reduces when $e = 13$ by Theorem 4.

$$p = 79,\ p(\beta) = 1 - \beta + \beta^{10}$$

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	$\sum a_i$
$-\beta^4 A$	−6	2	0	0	−2	−4	−2	−2	0	−4	−6	−3	−27
$-\beta^9 B$	0	−3	−5	−1	−6	−3	−1	−3	3	−1	−2	−5	−27
$-C$	−1	−5	−1	−4	−5	−5	1	1	−1	−4	1	−4	−27
$-\beta^6 D$	2	4	4	2	−3	0	3	0	−2	3	−3	2	12
$-\beta^{10} E$	4	3	8	3	4	4	4	8	8	4	7	7	64
$-\beta^3 F$	−2	−4	−5	1	−2	4	−1	−2	1	0	−4	0	−14

Since $\sum a_{i3} = -27$, (88) holds modulo 169 only when the three sums are all -27 or are 64, 12, -27, respectively. But the latter case gives $(0, 0) = -1$ and is excluded. Hence the first three rows of the table give the coefficients of $R(1, 1)$, $R(1, 2)$, $R(1, 3)$, while $(0, 0) = 2$.

$$p = 521, \quad p(\beta) = 1 + \beta - \beta^{12}$$

$-\beta^{11}A$	-2	4	-4	0	12	4	4	-6	16	8	7	8	51
$-\beta^{2}B$	18	11	18	4	4	0	6	10	6	2	16	8	103
$-C$	-15	-13	-15	-3	-13	-13	-17	-17	-15	-3	-17	-3	-144
$-\beta^{10}D$	4	-4	-16	0	-4	-8	-8	-10	-4	-19	-4	-6	-79
$-\beta^{8}E$	12	-12	-4	-6	-4	6	2	-5	-2	6	4	2	-1
$-\beta^{5}F$	-18	-10	-10	0	-5	-8	2	-6	-18	-12	-8	-12	-105

Since $\sum a_{i3} = -144$, (88) holds modulo 169 only when the first two sums are 51 and 103, or -79 and -1. The latter case gives $(0, 0) = +6$ and is to be excluded by other means such as (87).

$$p = 131, \quad p(\beta) = 1 - \beta + \beta^{11}$$

$-\beta^{3}A$	2	4	4	0	6	1	0	2	-6	2	4	6	25
$-\beta^{10}B$	5	-5	4	2	1	0	3	4	4	0	-2	-4	12
$-C$	-3	-5	-3	3	-5	-5	-4	-4	-3	3	-4	3	-27
$-\beta^{11}D$	-7	-3	1	-5	-3	-6	3	0	2	-1	-5	-3	-27
$-\beta E$	2	3	1	-2	-1	-2	0	2	2	2	9	-4	12
$-\beta^{12}F$	3	0	2	6	6	-6	1	-2	0	2	-1	1	12

Then (88) holds modulo 169 if the third sum is -27 only when the first sum is 25 and the second is 12.

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.