PERIOD EQUATIONS APPLIED TO DIFFERENCE SETS

EMMA LEHMER

Difference sets. A *difference set* of order k and multiplicity λ is a set of k elements $a_1, a_2, \cdots, a_k \pmod v$ such that the congruence

$$a_i - a_j \equiv d \pmod v$$

has exactly λ solutions for $d \not\equiv 0 \pmod v$.

A *multiplier* of a difference set is any number t such that the set $ta_1, ta_2, \cdots, ta_k$ is congruent to the set $a_1+s, a_2+s, \cdots, a_k+s$ in some order, for some value of s.

Hall and Ryser[1] proved the following interesting theorem:

Every prime divisor q of $k-\lambda$ is a multiplier provided $q>\lambda$. Although the proviso $q>\lambda$ is essential to the proof of the theorem, it appears that all divisors of $k-\lambda$ are actually multipliers in all the explicit numerical examples of difference sets which are available.

It therefore seems of interest to test this theorem out more generally on classes of known *residue difference sets*, that is, difference sets composed of nth power residues modulo a prime p. In this case we have shown [2] that:

The set of multipliers of a residue difference set is the set itself. Therefore any statement we can make about multipliers of a residue difference set will also be valid for the residues themselves and *vice versa*.

It is well known that the $(p-1)/2=k$ quadratic residues modulo a prime $p\equiv -1 \pmod 4$ form a difference set of multiplicity $\lambda=(p-3)/4$, so that $k-\lambda=(p+1)/4$. The validity of Hall and Ryser's theorem for all the divisors of $k-\lambda$ follows for these sets from the rather trivial theorem to the effect that:

THEOREM I. *All the divisors of $(p+z^2)/4$ are quadratic residues of $p\equiv -1 \pmod 4$, if z is odd.*

In the first place 2 divides $(p+z^2)/4$ only if $p\equiv -1 \pmod 8$, in which case 2 is a quadratic residue of p. If q is any odd divisor of $p+z^2$, then we can write $p+z^2=qm$ and by the law of quadratic reciprocity

$$\left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{qm - z^2}{q}\right) = \left(\frac{z^2}{q}\right) = 1.$$

Hence all the divisors of $(p+z^2)/4$ are quadratic residues of p.

Presented to the Society, June 19, 1954; received by the editors July 26, 1954.

Although it has been shown [2] that cubic residues do not form difference sets, Marshall Hall has constructed a set (as yet unpublished) made up of cubic residues and of sextic nonresidues belonging to a certain residue class. It can be shown that such a set actually forms a difference set of $(p-1)/2$ elements provided $p=4A^2+27$. In this case $k-\lambda=(p+1)/4$ and he was able to show by the law of cubic reciprocity that all the divisors of $k-\lambda$ are cubic residues and therefore multipliers. The consideration of the cubic equation for the trinomial periods gives a slightly more general theorem of which this is a special case, but which does not appear to follow from the law of cubic reciprocity.

THEOREM II. *If* $p=4A^2+27B^2$, *then all the divisors of* $(p+B^2)/4$ *are cubic residues of* p.

This theorem will be proved in the next section.

The corresponding results for quartic residues are as follows. Chowla [3] has shown that the $(p-1)/4=k$ quartic residues form a difference set of multiplicity $\lambda=(p-5)/16$ modulo a prime $p=1+4y^2$, y odd. Hence in this case $k-\lambda=(3p+1)/16$. In a previous paper [2] we have also considered a modified residue difference set for which zero was counted as an element of the set, and showed that the quartic residues and zero form a difference set modulo $p=9+4y^2$, y odd. In this case $k-\lambda=(3p+9)/16$. The fact that all the divisors of $k-\lambda$ are multipliers in both these cases follows from a theorem of Sylvester [4], which was stated by him without proof on several occasions and which is as follows:

THEOREM III (Sylvester). *If* $p=x^2+4y^2$, y *odd, then all the divisors of* $(3p+x^2)/16$ *are quartic residues of* p.

For proof he simply states: "This theorem deduced from the method applied to the divisors of period-functions does not appear to be referable to any known theorem concerning biquadratic residues." We hope that in our proof in the next section we have reconstructed the method that Sylvester had in mind.

Since, in our modified difference set, 3 is always a divisor of $k-\lambda$ we can state the following corollary to Theorem III.

COROLLARY I. 3 *is a quartic residue of all primes of the form* $p=9+4y^2$, y *odd.*

This corollary can be easily verified by the law of quartic reciprocity.

We have also shown [2] that the octic residues form a difference set

modulo $p=9+4y^2=1+2b^2$, with $k-\lambda=(7p+1)/64$, if 2 is a quartic residue, and that the octic residues and zero form a difference set, if 2 is a quartic residue, for $p=21^2+4y^2=7^2+2b^2$, in which case $k-\lambda=(7p+49)/64$. The fact that all the divisors of $k-\lambda$ are multipliers for both these classes of octic difference sets follows from the following theorem, whose proof will be found in the next section. Since the condition for quartic residuacity of 2 for $p\equiv 9 \pmod{16}$ is $y=4y_1$ this theorem can be stated:

THEOREM IV. *If* $p=9a^2+64y_1^2=a^2+2b^2\equiv 9 \pmod{16}$, *then all the divisors of* $(7p+a^2)/64$ *are octic residues of* p.

The special case of this theorem which corresponds to the modified residue set for which 7 is always a divisor of $k-\lambda$ leads to the following corollary:

COROLLARY II. 7 *is an octic residue of all primes of the form* $p=21^2+64y^2=7^2+2b^2$.

In general primes satisfying conditions of the theorem are rather rare; there are only three such primes less than ten thousand, namely $p=73$, 6361, and 9001. They may be found from the solutions of the Pell equation

$$t^2 - 2u^2 = a^2,$$

with $p=a^2+8t^2$, or from consulting a table of quadratic partitions of p such as Cunningham [5].

This disposes of all known residue difference sets and shows that for such sets *all the divisors of* $k-\lambda$ *are multipliers.*

Period equations. The proofs of Theorems 2, 3, and 4 are based on a theorem of Kummer concerning the divisors of numbers represented by equations whose roots are the so-called periods. If $p=ef+1$ is a prime, then the f-nomial periods $\eta_0, \eta_1, \cdots, \eta_{e-1}$ are given by

$$\eta_k = \sum_{\nu=0}^{f-1} \exp(2\pi i g^{e\nu+k}/p) \qquad (k = 0, 1, \cdots, e-1) \tag{1}$$

where g is a primitive root of p.

These η's satisfy an irreducible equation of degree e with integer coefficients and have the following well known properties

$$\sum_{\nu=0}^{e-1} \eta_\nu = -1, \tag{2}$$

$$\eta_m\eta_{m+k} = \sum_{h=0}^{e-1} (k, h)\eta_{m+h} + f\epsilon_k, \tag{3}$$

where

$$\epsilon_k = \begin{cases} 1 & \text{if } f \text{ is even, } k = 0, \text{ or if } f \text{ is odd, } k = e/2, \\ 0 & \text{otherwise,} \end{cases}$$

and where the cyclotomic integer (k, h) is the number of solutions of the congruence

$$g^{e\nu+k} + 1 \equiv g^{e\mu+h} \pmod{p} \qquad (\mu, \nu = 1, 2, \cdots, f)$$

having the property that

$$(k, h) = (h + e/2, k + e/2) \qquad (f \text{ odd}). \tag{4}$$

We shall denote by

$$\phi_e(y) = \prod_{i=0}^{e-1} (y - \eta_i) = 0 \tag{5}$$

the period equation of degree e. Kummer [6] introduces another quantity

$$P_r = \prod_{\nu=0}^{e-1} (\eta_\nu - \eta_{\nu+r}) \tag{6}$$

and states that "P, being a *symmetric* function of the periods, is an integer." This statement is questioned by Vandiver [7] and we take this opportunity to point out that although P is not a symmetric function of the periods it is nevertheless an integer, being a *cyclic* function of the periods, which is doubtless what Kummer had in mind. The fact that P_r is an integer is important in the proof of Kummer's theorem, which can now be stated as follows:

KUMMER'S THEOREM. *The form $\phi_e(y)$ has besides the divisor p, in general, only such primes for divisors which are eth power residues of p; besides this, however, it can have a finite number of exceptional divisors when e is composite. These exceptional prime divisors q are such that if g.c.d. $(r, e) = \alpha$ then the first α factors of the product P_r must be divisible by q, which in this case may be only an αth power residue of p.*

REMARK. It must be noted that the product of the first α factors of P_r need not be an integer and that in this case divisibility by q means divisibility of the coefficients of every η by q. Of course if P_r itself happens to be prime to $\phi_e(y)$ for all r which have a factor in common with e, there are no exceptional primes.

Period equations $\phi_e(y) = 0$ are well known [8] for $e = 2$, 3, and 4. The reduced equations $F_e(z) = 0$ with roots $\zeta_i = e\eta_i + 1$ are much simpler and easier to handle. The corresponding forms are connected by the relation

$$\phi_e(y) = e^{-e}F_e(z), \qquad z = ey + 1, \tag{7}$$

so that we shall be able to make statements about the character of the divisors of numbers represented by $F_e(z)/e^e$.

For $e=2$, ζ_0 is the well known Gauss sum, and for $p \equiv -1 \pmod 4$

$$F_2(z) = z^2 + p = 0. \tag{8}$$

Hence by Kummer's theorem all the divisors of $(z^2+p)/4$, with z odd, are quadratic residues of p, which gives another proof of our Theorem I.

For $e=3$ and $p=4A^2+27B^2$, the trinomial period equation may be written

$$F_3(z) = z^3 - 3px - 4pA = 0, \qquad A \equiv 1 \pmod 3. \tag{9}$$

Letting $z=A$, we have

$$F_3(A) = A^3 - 7pA = A(A^2 - 7p) = A\left(\frac{p - 27B^2}{4} - 7p\right) \tag{10}$$

$$= -27A(p + B^2)/4.$$

Hence, since e is a prime, it follows from Kummer's theorem that all the divisors of A and of $(p+B^2)/4$ are cubic residues of p without exceptions. This proves our Theorem II.

For $e=4$ and $p=x^2+4y^2$, y odd, the period equation can be best written in a form given by Lebesgue [8], namely

$$F_4(z) = (z^2 + 3p)^2 - 4p(z - x)^2 = 0, \qquad x \equiv 1 \pmod 4. \tag{11}$$

Letting $z=x$, we obtain at once

$$F_4(x) = (3p + x^2)^2. \tag{12}$$

Hence by Kummer's theorem all the divisors of $(3p+x^2)/16$ are quartic residues of p provided they are prime to

$$P_2 = (\eta_0 - \eta_2)^2(\eta_1 - \eta_3)^2 = py^2. \tag{13}$$

This is always the case because $(3p+x^2)/16=(p-y^2)/4$ is prime to py^2. This value for P_2 can be found in a footnote of Sylvester's note [4, p. 478] and can be easily calculated from the quartic equation (11).

For $e=8$, $p=x^2+64y_1^2=a^2+2b^2\equiv 9 \pmod{16}$, which is the case under consideration, the period equation has never been calculated. This is one of four possible cases (for which 2 is a quartic residue), which arise with $e=8$, none of which has been explicitly written out. To quote Smith's *Report* [8]: "The determination of the coefficients

of $F(y)=0$ may be effected for any given prime p and for any divisor e of $p-1$ by methods which, however tedious, present no theoretical difficulty." We shall now proceed with this task for a fairly general class of primes p.

To simplify the calculations we shall first determine the equation of degree 4 whose roots are $\zeta_0, \zeta_2, \zeta_4, \zeta_6$. This equation turns out to be of the form

$$f(z) = L(z) + p^{1/2}M(z) = 0$$

where $L(z)$ and $M(z)$ are polynomials with integer coefficients. It follows that the remaining 4 roots satisfy the equation $L(z)-p^{1/2}M(z)=0$ so that

$$F_e(z) = [L(z)]^2 - p[M(z)]^2 = 0. \tag{14}$$

This will give our octic equation in a form similar to Lebesgue's quartic. Hence we need only calculate the coefficients of

$$\begin{aligned} f(z) &= (z-\zeta_0)(z-\zeta_2)(z-\zeta_4)(z-\zeta_6) \\ &= z^4 - c_1z^3 + c_2z^2 - c_3z + c_4 = 0. \end{aligned} \tag{15}$$

To do this we refer to Lebesgue's form of the quartic [8], which for $p\equiv 1 \pmod 4$ is as follows

$$\begin{aligned} F_4(z) &= (z^2-p)^2 - 4p(z-x)^2 \\ &= [z^2 - 2p^{1/2}z + (2p^{1/2}x - p)][z^2 + 2p^{1/2}z - (2p^{1/2}x + p)]. \end{aligned} \tag{16}$$

Thus the quantities

$$\alpha = (\zeta_0 + \zeta_4)/2 \quad \text{and} \quad \beta = (\zeta_2 + \zeta_6)/2$$

are roots of the quadratic

$$z^2 - 2p^{1/2}z + (2p^{1/2}x - p) = 0,$$

and hence

$$c_1 = \zeta_0 + \zeta_2 + \zeta_4 + \zeta_6 = 2(\alpha + \beta) = 4p^{1/2}. \tag{17}$$

We shall also need the following expressions:

$$\begin{aligned} \alpha\beta = 2p^{1/2}x - p, \qquad \alpha^2 + \beta^2 = 6p - 4p^{1/2}x, \\ \alpha^3 + \beta^3 = 2p^{1/2}(7p - 6p^{1/2}x). \end{aligned} \tag{18}$$

Next

$$c_2 = 4\alpha\beta + \zeta_0\zeta_4 + \zeta_2\zeta_6 = 8p^{1/2}x - 4p + \zeta_0\zeta_4 + \zeta_2\zeta_6. \tag{19}$$

We proceed to calculate

$$\zeta_0\zeta_4 = 64\eta_0\eta_4 + 8(\eta_0 + \eta_4) + 1. \tag{20}$$

By (3) and (4)

$$\begin{aligned} 64\eta_0\eta_4 = {} & (\eta_0 + \eta_4)64(0, 0) + (\eta_1 + \eta_5)64(1, 0) \\ & + (\eta_2 + \eta_6)64(2, 0) + (\eta_3 + \eta_7)64(3, 0) + 8(p - 1). \end{aligned} \tag{21}$$

The cyclotomic numbers (0, 0), (1, 0), (2, 0), and (3, 0) of order 8 are known [9] to be as follows:

$$\begin{aligned} 64(0, 0) = p - 15 - 2x, \qquad & 64(2, 0) = p - 7 - 2x - 8a, \\ 64(1, 0) = 64(3, 0) = p - 7 + 2x + 4a. & \end{aligned} \tag{22}$$

Hence

$$\begin{aligned} \zeta_0\zeta_4 = {} & (\eta_0 + \eta_2 + \eta_4 + \eta_6)(p - 7 - 2x) \\ & + (\eta_1 + \eta_3 + \eta_5 + \eta_7)(p - 7 + 2x + 4a) \\ & - 8a(\eta_2 + \eta_6) + 8p - 7. \end{aligned} \tag{23}$$

But

$$\begin{aligned} (\eta_0 + \eta_2 + \eta_4 + \eta_6) &= (p^{1/2} - 1)/2, \\ (\eta_1 + \eta_3 + \eta_5 + \eta_7) &= -(p^{1/2} + 1)/2 \end{aligned} \tag{24}$$

so that

$$\begin{aligned} \zeta_0\zeta_4 &= 7p - 2a - 2p^{1/2}(x + a) - 8a(\eta_2 + \eta_6) \\ &= 7p - 2p^{1/2}(x + a) - 2a\beta. \end{aligned} \tag{25}$$

Similarly

$$\begin{aligned} \zeta_2\zeta_6 &= 7p - 2a - 2p^{1/2}(x + a) - 8a(\eta_0 + \eta_4) \\ &= 7p - 2p^{1/2}(x + a) - 2a\alpha. \end{aligned} \tag{26}$$

Adding,

$$\zeta_0\zeta_4 + \zeta_2\zeta_6 = 14p - 4p^{1/2}(x + a) - 4ap^{1/2} = 14p - 4p^{1/2}(x + 2a). \tag{27}$$

Hence by (19)

$$c_2 = 10p + 4p^{1/2}(x - 2a). \tag{28}$$

We can now write

$$c_3 = 2\zeta_0\zeta_4\beta + 2\zeta_2\zeta_6\alpha. \tag{29}$$

Using (25) and (26) we have

$$c_3 = [7p - 2p^{1/2}(x + a)]4p^{1/2} - 4a(\alpha^2 + \beta^2). \tag{30}$$

Hence by (18) and (30)

$$c_3 = 4p^{1/2}(7p + 4ax) - 8p(x + 4a). \tag{31}$$

Finally by (25) and (26)

$$\begin{aligned} c_4 = \zeta_0\zeta_4 \cdot \zeta_2\zeta_6 = {} & [7p - 2p^{1/2}(x + a)]^2 \\ & -4a[7p - 2p^{1/2}(x + a)]p^{1/2} + 4a^2\alpha\beta. \end{aligned}$$

Hence by (18)

$$c_4 = 49p^2 + 4p(x^2 + 4ax + 2a^2) + p^{1/2}(8a^2x - 28p(x + 2a)). \tag{32}$$

Hence substituting (17), (28), (31), and (32) into (15) we obtain

$$\begin{aligned} F_8(z) = {} & [(z^2 + 7p)^2 - 4p(z^2 - 2(x + 4a))z - (x^2 + 4ax + 2a^2)]^2 \\ & - 16p[-z^3 + (x - 2a)z^2 - (7p + 4ax)z \\ & + (2a^2x - 7px - 14pa)]^2 = 0. \end{aligned} \tag{33}$$

In order to apply this result to the proof of Theorem IV we first simplify it by considering the special case $x = -3a$ and denote the corresponding equation by $F_8^*(z) = 0$. This produces a considerable simplification, namely

$$\begin{aligned} F_8^*(z) = {} & [(z^2 + 7p)^2 - 4p(z - a)^2]^2 \\ & - 16p[(z - a)(z^2 + 6az - 6a^2 + 7p)]^2 = 0. \end{aligned}$$

It is now quite evident that

$$F_8^*(a)/8^8 = [(a^2 + 7p)/64]^2, \tag{34}$$

and hence by Kummer's theorem all the divisors of $(a^2+7p)/64$ must be octic residues of p provided they are prime to P_2 and P_4.

We next calculate P_4:

$$8^8P_4 = (\zeta_0 - \zeta_4)^2(\zeta_1 - \zeta_5)^2(\zeta_2 - \zeta_6)^2(\zeta_3 - \zeta_7)^2. \tag{35}$$

We can write the product of two of these factors as follows:

$$\begin{aligned} (\zeta_0 - \zeta_4)^2(\zeta_2 - \zeta_6)^2 &= 16(\alpha^2 - \zeta_0\zeta_4)(\beta^2 - \zeta_2\zeta_6) \\ &= 16[(\alpha\beta)^2 - (\alpha^2\zeta_2\zeta_6 + \beta^2\zeta_0\zeta_4) + c_4]. \end{aligned} \tag{36}$$

By (18), (25), (26), and (32) we have

$$\begin{aligned} & (\zeta_0 - \zeta_4)^2(\zeta_2 - \zeta_6)^2 \\ & \quad = 16[(2p^{1/2}x - p)^2 - (7p - 2p^{1/2}(x + a))(6p - 4p^{1/2}x) \\ & \quad + 4ap^{1/2}(7p - 6p^{1/2}x) + 49p^2 + 4p(x^2 + 4ax + 2a^2) \\ & \quad + p^{1/2}(8a^2x - 28p(x + 2a))]. \end{aligned}$$

Combining we get

$$(\zeta_0 - \zeta_4)^2(\zeta_2 - \zeta_6)^2 = 128[p(p + a^2 - 2ax) + p^{1/2}(px - 2pa + a^2x)]. \tag{37}$$

Similarly

$$(\zeta_2 - \zeta_5)^2(\zeta_3 - \zeta_7)^2 = 128[p(p + a^2 - 2ax) - p^{1/2}(px - 2pa + a^2x)]. \tag{38}$$

Multiplying these together we have

$$\begin{aligned} 8^8P_4 &= 128^2[p^2(p + a^2 - 2ax)^2 - p(px - 2pa + a^2x)^2] \\ &= 128^2p(p - x^2)(p - a^2)^2 = 2^{22}y_1^2b^4p. \end{aligned} \tag{39}$$

Remembering that b is even, $b=2b_1$, we finally have

$$P_4 = 4y_1^2b_1^4p. \tag{40}$$

Since P_4 and $(7p+a^2)/64$ cannot have an odd factor in common, there are no odd exceptional divisors which are quartic instead of octic residues. As for the character of 2, it is well known [10] that 2 is an octic residue of $p\equiv 9 \pmod{16}$ if and only if y is odd. If y is even, however, then $p\equiv x^2\equiv 9a^2 \pmod{256}$ and therefore $(7p+a^2)/64\equiv a^2$ is not divisible by 2. Hence there are no exceptional divisors of P_4. It remains to inquire if there are divisors of $7p+a^2$ which may be only quadratic residues of p. Such exceptional divisors would have to divide the coefficients of the expansion of the product of the first 2 factors of P_2 by Kummer's theorem, namely

$$\begin{aligned} &(\eta_0 - \eta_2)(\eta_1 - \eta_3) \\ &\quad = [(-2a + b)\eta_0 + (2a - b)\eta_1 + (2a + b)\eta_2 - (2a + b)\eta_3 \\ &\quad + \quad (2a + b + 2y)\eta_4 + (-2a + b - 2y)\eta_5 \\ &\qquad\quad + (-2a - b + 2y)\eta_6 + (2a - b - 2y)\eta_7]/4. \end{aligned} \tag{41}$$

These coefficients have obviously no odd common factor, which completes the rather lengthy proof of Theorem IV.

It may be interesting to note that P_2 itself contains the factor $(7p+a^2)/64$. In fact we find that for $x\equiv -3a$

$$P_2 = \left(\frac{7p + a^2}{64}\right)^2 py^2$$

and that

$$P_1 = \left(\frac{7p + a^2}{64}\right)\left(\frac{9p - 17a^2}{16} - by\right)py_1^2,$$

$$P_3 = \left(\frac{7p + a^2}{64}\right)\left(\frac{9p - 17a^2}{16} + by\right)py_1^2.$$

From this we can write down the discriminant Δ of the octic $\phi_8(y)$ as $P_1^2P_2^2P_3^2P_4$.

$$\Delta = 2^{10}\left[\frac{7p + a^2}{64}\right]^8\left[\left(\frac{9p - 17a^2}{16}\right)^2 - b^2y^2\right]^2 y_1^{14}b_1^4p^7$$

$$= 2^{18}(a^2 + 7y_1^2)^8[(a^2 + 9y_1^2)^2 - 4b_1^2y_1^2]^2 y_1^{14}b_1^4p^7.$$

For example, for $p = 73$, this discriminant is

$$\Delta = 2^{54} \cdot 3^4 \cdot 73^7.$$

Bibliography

1. Marshall Hall, Jr. and H. J. Ryser, *Cyclic incidence matrices*, Canadian Journal of Mathematics vol. 4 (1951) pp. 495–502.

2. Emma Lehmer, *On residue difference sets*, Canadian Journal of Mathematics vol. 5 (1952) pp. 425–432.

3. S. Chowla, *A property of biquadratic residues*, Proceedings of the National Academy of Sciences, India, Sec. A vol. 14 (1944) pp. 45–46.

4. J. J. Sylvester, *Mathematical papers*, vol. 3, Cambridge, 1909, pp. 448, 477–478, 480.

5. A. Cunningham, *Quadratic partitions*, London, 1904.

6. E. E. Kummer, Journal für Mathematik vol. 30 (1846) pp. 107–116.

7. Bulletin of the National Research Council vol. 5 no. 28 (1923) p. 54.

8. H. J. S. Smith, *Collected papers*, vol. 1, p. 103.

9. Emma Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod{p}$, Pacific Journal of Mathematics vol. 5 (1955) pp. 103–118.

10. A. E. Western, *Some criteria for the residues of eighth and other powers*, Proc. London Math. Soc. (2) vol. 9 (1911) pp. 244–272.

Berkeley, Calif.