PACIFIC JOURNAL OF MATHEMATICS
Vol. 82, No. 1, 1979

A COMBINATORIAL PROBLEM IN FINITE FIELDS, I

GERALD MYERSON

Given a subgroup G of the multiplicative group of a finite field, we investigate the number of representations of an arbitrary field element as a sum of elements, one from each coset of G. When G is of small index, the theory of cyclotomy yields exact results. For all other G, we obtain good estimates.

This paper formed a portion of the author's doctoral dissertation.

Let $p = 2n + 1$ be an odd prime. Consider the 2^n sums represented by the expression

$$\pm 1 \pm 2 \pm 3 \pm \cdots \pm n .$$

How do these sums distribute themselves among the residue classes modulo p? The answer is, as uniformly as possible; in fact, if we define $N(a)$ as the number of ways of choosing the signs so that $\pm 1 \pm 2 \pm \cdots \pm n \equiv a \pmod p$ then we have

THEOREM 1.

$$N(a) = \frac{1}{p}\left(2^n - \left(\frac{2}{p}\right)\right) \text{ for } a \neq 0 \pmod p ,$$
$$N(0) = \frac{1}{p}\left(2^n - \left(\frac{2}{p}\right)\right) + \left(\frac{2}{p}\right) .$$

Here $(2/p)$ is the Legendre symbol, that is,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } 2 \text{ is a quadratic residue} \pmod p \\ -1 \text{ if } 2 \text{ is not a quadratic residue} \pmod p . \end{cases}$$

Our proof of Theorem 1 will rest on the following lemmas.

LEMMA 2. *If $ab \not\equiv 0 \pmod p$ then $N(a) = N(b)$.*

Proof. Assume $\sum_{k=1}^n u_k k \equiv a \pmod p$, with $u_k \in \{1, -1\}$. Since $ab \not\equiv 0 \pmod p$ there is a c such that $ac \equiv b \pmod p$. Thus we have $\sum_{k=1}^n u_k ck \equiv b \pmod p$. Now for $k = 1, 2, \cdots, n$, let $ck \equiv u_k' m_k \pmod p$, where $1 \leq m_k \leq n$, $u_k' \in \{1, -1\}$; these conditions determine m_k and u_k' uniquely. Thus,

$$b \equiv \sum_{k=1}^n u_k ck \equiv \sum_{k=1}^n u_k u_k' m_k \equiv \sum_{k=1}^n u_k'' m_k \pmod p ,$$

with

$$u_k'' \in \{1, -1\} .$$

Now, the m_k are all distinct: if $m_k = m_h$, then $ck \equiv \pm ch \pmod p$, so $k \equiv \pm h \pmod p$, so $k = h$ (since $1 \leqq k \leqq n, 1 \leqq h \leqq n$). Therefore, $b \equiv \sum_{k=1}^{n} u_k'' m_k \pmod p$ is a representation of b, corresponding to our original representation of a. Multiplication by c', where $cc' \equiv 1 \pmod p$, returns us to the original representation of a. We have established a one-to-one correspondence between the set of representations of a and the set of representations of b, and this shows that $N(a)$ is independent of a for $a \not\equiv 0 \pmod p$.

Now let N denote the common value of $N(a)$, $a \not\equiv 0 \pmod p$, and note that

$$N(0) + (p-1)N = 2^n$$

by counting the total number of expressions two different ways. We now obtain a second linear relation between $N(0)$ and N through the use of a generating function. Let θ be any primitive pth root of unity.

LEMMA 3. $\prod_{k=1}^{n} (\theta^k + \theta^{-k}) = \sum_{a=0}^{p-1} N(a)\theta^a = N(0) - N$.

Proof. In expanding the product into a sum of powers of θ each term is of the form $\theta^{\pm 1 \pm 2 \pm \cdots \pm n}$. The number of occurrences of θ^a, $0 \leqq a \leqq p-1$, is therefore the number of choices of signs for which $\pm 1 \pm 2 \pm \cdots \pm n \equiv a \pmod p$, which is $N(a)$. This proves the first equality. The second follows from Lemma 2 and the observation that $\sum_{a=0}^{p-1} \theta^a = 0$.

If we can evaluate $\prod_{k=1}^{n} (\theta^k + \theta^{-k})$ then we will have two equations for $N(0)$ and N.

LEMMA 4.

$$\prod_{k=1}^{n} (\theta^k + \theta^{-k}) = \left(\frac{2}{p}\right) .$$

Proof. $\theta + \theta^{-1}$ is a unit in the ring of integers in $Q(\theta)$; in fact, $(\theta + \theta^{-1})(\theta + \theta^5 + \theta^9 + \cdots + \theta^{2p-1}) = 1$. The numbers $\theta^k + \theta^{-k}$ are conjugate to $\theta + \theta^{-1}$, thus are also units; hence, $\prod_{k=1}^{n} (\theta^k + \theta^{-k})$ is a unit. By Lemma 3 this product is a rational integer, hence it must be 1 or -1. We have

$$\prod_{k=1}^{n} (\theta^k + \theta^{-k}) = N(0) - N\,, \quad \text{(Lemma 3)}$$

$$N(0) - N \equiv N(0) + (p-1)N \pmod p\,,$$

$$N(0) + (p-1)N = 2^n\,,$$

$$2^n \equiv \left(\frac{2}{p}\right) \pmod p \quad \text{(Euler's criterion)}.$$

Thus $\prod_{k=1}^{n} (\theta^k + \theta^{-k}) \equiv (2/p) \pmod p$; but since the product must equal 1 or -1, it follows that $\prod_{k=1}^{n} (\theta^k + \theta^{-k}) = (2/p)$.

Proof of Theorem 1. We now have two linear equations in $N(0)$ and N;

$$N(0) + (p-1)N = 2^n\,,$$

$$N(0) - N = \left(\frac{2}{p}\right),$$

where the second equation is a consequence of Lemmas 3 and 4. Simultaneous solution of these equations yields Theorem 1.

We now present a generalization of the problem solved above; the remainder of this paper is an attempt to solve the generalized problem. We fix the following notation: e and f are positive integers such that $ef + 1 = q = p^\alpha$ is a prime power, and F_q is the field of q elements. The multiplicative group of units of F_q, denoted F_q^x, is generated by the primitive element g. The subgroup G, consisting of all the eth powers in F_q^x, is generated by g^e. The cosets of G in F_q^x are denoted and defined by $G_k = g^k G$, $k = 0, 1, \cdots, e-1$. In particular, $G_0 = G$. For each $x \in F_q$ define $N(x)$ to be the number of solutions of $\sum_{k=0}^{e-1} s_k = x$, with $s_k \in G_k$; that is, $N(x)$ is the number of representations of x as a sum of elements, taking precisely one from each coset. $N(x)$ depends, of course, not only on x but on e and f as well; it is, however, independent of the choice of the generator for F_q^x.

With this notation, our problem is, find $N(x)$.

We note that the case $e = (p-1)/2$, $f = 2$, where p is prime, is our original problem; if $e = (p-1)/2$ then $g^e = -1$, $G = \{1, -1\}$, and the cosets of G are the sets $\{k, -k\}$, $k = 1, 2, \cdots, (p-1)/2$.

We now try to solve our new problem by following the solution of the old one. We first note that if $s_k \in G_k$ and $s_h \in G_h$ then $s_k^{-1} \in G_{-k}$ and $s_k s_h \in G_{k+h}$, where the subscripts are to be reduced mod e.

LEMMA 5. *If $xy \neq 0$, then $N(x) = N(y)$.*

Proof. Assume $\sum_{k=1}^{e-1} s_k = x$, $s_k \in G_k$. Since $xy \neq 0$ there is a $z \in F_q^x$ such that $xz = y$. Thus, $\sum_{k=0}^{e-1} zs_k = y$. But multiplication by z merely permutes the cosets G_k, so this gives a representation of y. Multiplication by z', where $zz' = 1$, returns us to the original representation of x, so we have a one-one correspondence between the two sets of representations.

Now let N denote the common value of $N(x)$, $x \neq 0$, and note that

$$N(0) + (q-1)N = f^e , \tag{1}$$

by counting the number of sums $\sum_{k=0}^{e-1} s_k$, $s_k \in G_k$, in two different ways.

To generalize Lemma 3 we need an analogue for the expressions $\theta^k + \theta^{-k}$. Letting θ be a primitive complex pth root of unity we define the *periods* $\eta_k = \sum_{x \in G_k} \theta^{Trx}$, $k = 0, 1, \cdots, e-1$. Here Tr is the trace map, $Tr: F_q \to F_p$; the elements of $F_p \simeq Z/pZ$ are identified with representatives of the cosets of pZ in Z; the value of θ^{Trx} is independent of the choice of representative since $\theta^p = 1$. We note that η_k depends on the parameters e and f, and also on g: a different choice of g would permute the η_k among themselves. Note that in the case $q=p$ we can simply define $\eta_k = \sum_{a \in G_k} \theta^a$, $k=0, 1, \cdots, e-1$. In particular, if $f = 2$ the periods are seen upon renumbering to be the numbers $\eta_k = \theta^k + \theta^{-k}$ of our previous discussion.

LEMMA 6. $\prod_{k=0}^{e-1} \eta_k = \sum_{x \in F_q} N(x)\theta^{Trx} = N(0) - N$.

Proof. In expanding the product into a sum of powers of θ each term is of the form, $\theta^{Tr(s_1+s_2+\cdots+s_{e-1})}$, $s_k \in G_k$. The number of occurrences of θ^{Trx} is therefore the number of representations of x as $\sum_{k=0}^{e-1} s_k$, $s_k \in G_k$, which is $N(x)$. This proves the first equality. The second follows from Lemma 5 and the observation that

$$\sum_{x \in F_q} \theta^{Trx} = 0 .$$

Lemma 6 gives a linear relation between $N(0)$ and N which, together with (1), can be used to evaluate $N(0)$ and N if we can evaluate $\prod_{k=0}^{e-1} \eta_k$. For fixed values of e, it is often possible to obtain formulas for $\prod_{k=0}^{e-1} \eta_k$ using the theory of cyclotomy.

In the next section, we give the definitions and quote the theorems we need from cyclotomy. The reader is referred to [7] for a detailed exposition with proofs.

Cyclotomy. We begin by defining the cyclotomic constants.

DEFINITION. The cyclotomic constant (k, h) is the number of elements $s \in G_k$ such that $1 + s \in G_h$.

The constants (k, h) depend on our parameters e and f; also, a different choice of generator g, by permuting the cosets G_k, will permute the constants (k, h). Their importance in the problem under consideration stems from the next two propositions.

PROPOSITION 7. *$\eta_0\eta_k = \sum_{h=0}^{e-1}(k, h)\eta_h + fn_k$, where n_k is defined by*

$$n_0 = 1 \text{ if } f \text{ is even },$$
$$n_0 = 1 \text{ if } p = 2 ,$$
$$n_{e/2} = 1 \text{ if } f \text{ and } p \text{ are odd },$$
$$n_k = 0 \text{ in all other cases }.$$

PROPOSITION 8. *$\eta_m\eta_{m+k} = \sum_{h=0}^{e-1}(k, h)\eta_{m+h} + fn_k$, where the subscripts are to be interpreted modulo e.*

Repeated applications of Propositions 7 and 8 will enable us to evaluate $\Pi\eta_k$, provided we know the constants (k, h).

The constants are given, in the cases $e = 2, 3$, and 4, by the following theorems.

PROPOSITION 9. (*Dickson* [3, p. 48]). *Assume $e = 2$.*

If f is even, the cyclotomic matrix $M^{(2)}$ is given by $M^{(2)} = \begin{pmatrix} A & B \\ B & B \end{pmatrix}$, where $4A = q - 5$, $4B = q - 1$.

If f is odd, $M^{(2)} = \begin{pmatrix} A & B \\ A & A \end{pmatrix}$, where $4A = q - 3, 4B = q + 1$.

PROPOSITION 10. (*Storer* [7, p. 35]). *Let $e = 3$. Let c and d be defined by $4q = c^2 + 27d^2$, $c \equiv 1 \pmod 3$, and, if $p \equiv 1 \pmod 3$, then $(c, p) = 1$; these restrictions determine c uniquely, and d up to sign. Then*

$$M^{(3)} = \begin{pmatrix} A & B & C \\ B & C & D \\ C & D & B \end{pmatrix}, \text{ where } \begin{aligned} 9A &= q - 8 + c , \\ 18B &= 2q - 4 - c - 9d , \\ 18C &= 2q - 4 - c + 9d , \\ 9D &= q + 1 + c . \end{aligned}$$

PROPOSITION 11. (*Storer* [7, pp. 48, 51]). *Let $e = 4$. Let s and t be defined by $q = s^2 + 4t^2$, $s \equiv 1 \pmod 4$, and, if $p \equiv 1 \pmod 4$, then $(s, p) = 1$; these restrictions determine s uniquely, and t up to sign.*

If f is even, then

$$M^{(4)} = \begin{pmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{pmatrix} \quad where \quad \begin{aligned} 16A &= q - 11 - 6s\ , \\ 16B &= q - 3 + 2s + 8t\ , \\ 16C &= q - 3 + 2s\ , \\ 16D &= q - 3 + 2s - 8t\ , \\ 16E &= q + 1 - 2s\ . \end{aligned}$$

If f is odd, then

$$M^{(4)} = \begin{pmatrix} A & B & C & D \\ E & E & B & D \\ A & E & A & E \\ E & D & B & E \end{pmatrix} \quad where \quad \begin{aligned} 16A &= q - 7 + 2s\ , \\ 16B &= q + 1 + 2s + 8t\ , \\ 16C &= q + 1 - 6s\ , \\ 16D &= q + 1 + 2s - 8t\ , \\ 16E &= q - 3 - 2s\ . \end{aligned}$$

Solutions in the cases $e = 2, 3, 4$.

We can now evaluate $\Pi\eta_k$, $N(0)$, and N in the cases $e = 2, 3, 4$.

THEOREM 12. *Let $e = 2$. If f is even, then*

$$\eta_0\eta_1 = -\frac{q-1}{4},\ N(0) = 0,\ N = \frac{q-1}{4}\ .$$

If f is odd, then

$$\eta_0\eta_1 = \frac{q+1}{4},\ \ N(0) = \frac{q-1}{2},\ \ N = \frac{q-3}{4}\ .$$

THEOREM 13. *Let $e = 3$. Let c be defined by $4q = c^2 + 27d^2$, $c \equiv 1 \pmod 3$, and, if $p \equiv 1 \pmod 3$, then $(c, p) = 1$. Then*

$$\eta_0\eta_1\eta_2 = \frac{1}{27}((c+3)q - 1)\ ,$$

$$N(0) = \frac{1}{27}(q + 1 + c)(q - 1)\ ,$$

$$N = \frac{1}{27}(q^2 - 3q - c)\ .$$

THEOREM 14. *Let $e = 4$. Let s be defined by $q = s^2 + 4t^2$, $s \equiv 1 \pmod 4$, and, if $p \equiv 1 \pmod 4$, then $(s, p) = 1$. If f is even, then*

$$\eta_0\eta_1\eta_2\eta_3 = \frac{1}{256}(q^2 - (4s^2 - 8s + 6)q + 1) = \frac{1}{256}((q-1)^2 - 4q(s-1)^2)\ ,$$

$$N(0) = \frac{1}{256}(q - 1)(q - 3 + 2s)(q + 1 - 2s)\ ,$$

$$N = \frac{1}{256}(q^3 - 4q^2 + 5q + 4s^2 - 8s + 2) .$$

If f is odd, then

$$\eta_0\eta_1\eta_2\eta_3 = \frac{1}{256}(9q^2 - (4s^2 - 8s - 2)q + 1) = \frac{1}{256}((3q+1)^2 - 4q(s-1)^2) ,$$

$$N(0) = \frac{1}{256}(q - 1)(q + 5 - 2s)(q + 1 + 2s) ,$$

$$N = \frac{1}{256}(q^3 - 4q^2 - 3q + 4s^2 - 8s - 6) .$$

Proof. Straightforward calculation yields the results on $\Pi\eta_k$. We present the case $e = 3$ as an example.

By Propositions 7 and 10, we have $\eta_0\eta_1 = B\eta_0 + C\eta_1 + D\eta_2$, whence

$$\begin{aligned}(\eta_0\eta_1)\eta_2 &= B(\eta_0\eta_2) + C(\eta_1\eta_2) + D(\eta_2)^2 \\ &= B(C\eta_0 + D\eta_1 + B\eta_2) + C(D\eta_0 + B\eta_1 + C\eta_2) + D(B\eta_0 + C\eta_1 + A\eta_2 + f) \\ &= (BC + CD + BD)\eta_0 + (BD + BC + CD)\eta_1 + (B^2 + C^2 + AD)\eta_2 + fD .\end{aligned}$$

Substituting for A, B, C, and D the values given in Proposition 10, and simplifying via $4q = c^2 + 27d^2$, we find

$$\begin{aligned}27\eta_0\eta_1\eta_2 &= (q^2 - 3q - c)(\eta_0 + \eta_1 + \eta_2) + (q^2 - 1 + cq - c) \\ &= -(q^2 - 3q - c) + (q^2 - 1 + cq - c) \\ &= (c + 3)q - 1 .\end{aligned}$$

The results an $N(0)$ and N then follow from the simultaneous solution of

$$N(0) + (q - 1)N = f^e ,$$

$$N(0) - N = \prod_{k=0}^{e-1} \eta_k .$$

Some special results and some approximations. We present two results of a more specialized nature.

THEOREM 15. *If q and f are both odd then $N(0) > N$.*

Proof. If q and f are both odd then $-1 \in G_{e/2}$. Thus for any k, $0 \leqq k < e/2$, $x \in G_k$ if and only if $-x \in G_{k+e/2}$. Then

$$\eta_{k+e/2} = \sum_{x \in G_{k+e/2}} \theta^{Trx} = \sum_{x \in G_k} \theta^{Tr(-x)} = \sum_{x \in G_k} \theta^{-Trx} = \bar{\eta}_k ,$$

where the overbar indicates complex conjugation. It follows that

$$\prod_{k=0}^{e-1} \eta_k = \prod_{k=0}^{e/2-1} \eta_k \bar{\eta}_k = \prod_{k=0}^{e/2-1} |\eta_k|^2 > 0 .$$

But by Lemma 6, $N(0) = N + \prod_{k=0}^{e-1} \eta_k$.

THEOREM 16. *Let $e = 4$. If $q - 1$ is a square, then $N(0) - N$ is a square.*

Proof. By hypothesis, $q = 1 + 4t^2$: thus, we can take $s = 1$ in Theorem 14. If f is even then

$$N(0) - N = \prod_{k=0}^{3} \eta_k = \left(\frac{q-1}{16}\right)^2 ;$$

if f is odd then

$$N(0) - N = \prod_{k=0}^{3} \eta_k = \left(\frac{3q+1}{16}\right)^2 .$$

Estimates for $\Pi\eta_k$ and $N(x)$. Cyclotomy for $e > 4$ has been of continuing interest to mathematicians. The reader is referred to [2] for the cases $e = 5, 6$, and 8; also to [9], [10], [4], [8], [1], and [5], for the cases $e = 10, 12, 14, 16, 18$, and 20, respectively. In each of these only the case $q = p$ is discussed. When the problems of cyclotomy have been solved for a given value of e, the methods of the proof of Theorem 13 will evaluate $\Pi\eta_k$ – see, e.g., [6], for the case $e = 5, q = p$. The computations involved are ghastly, as the reader can convince himself by inspecting the references cited above. The author feels that the importance of finding exact expressions for N and $N(0)$ is not sufficient to justify performing these computations. We present instead approximations to N and $N(0)$, based upon a lemma from cyclotomy.

LEMMA 17. (a) *If either f or p is even, then*

$$\sum_{k=0}^{e-1} \eta_k^2 = q - f .$$

(b) *If f and p are both odd, then*

$$\sum_{k=0}^{e-1} \eta_k \eta_{k+e/2} = q - f .$$

Proof. These are both special cases of Lemma 9 in [7].

LEMMA 18. (a) *If either f or p is even then η_k is real, $k = 0, 1, \cdots, e-1$.*

(b) *If f and p are both odd then $\eta_k \eta_{k+e/2}$ is real and positive,*

$k = 0, 1, \cdots, e-1$.

Proof. (a) If f is even then $-1 \in G_0$. Thus if $x \in G_k$ then $-x \in G_k$, and $x \neq -x$. Hence, if θ^{Trx} appears in η_k, so does $\theta^{Tr(-x)} = \theta^{-Trx}$. Thus, η_k is real. If p is even then $p=2$. Thus $\theta = -1$ and η_k is real.

(b) This was shown in the proof of Theorem 15.

THEOREM 19. $|\prod_{k=0}^{e-1} \eta_k| \leqq ((q-f)/e)^{e/2}$; $|N(0) - f^e/q| \leqq ((q-f)/e)^{e/2}$; $|N - f^e/q| \leqq q^{-1}((q-f)/e)^{e/2}$.

Proof. If either f or p is even then $\sum_{k=0}^{e-1} \eta_k^2 = q - f$. If both f and p are odd then $\sum_{k=0}^{e-1} \eta_k \eta_{k+e/2} = q - f$. In either case we may, by Lemma 18, apply the inequality of the arithmetic and geometric means. We obtain $\prod_{k=0}^{e-1} \eta_k^2 \leqq ((q-f)/e)^e$, or $|\prod_{k=0}^{e-1} \eta_k| \leqq ((q-f)/e)^{e/2}$.

The other two inequalities follow from the first and from the relations $N(0) + (q-1)N = f^e$, $N(0) - N = \prod_{k=0}^{e-1} \eta_k$.

The reader is encouraged to compare the approximations of Theorem 19 with the exact results of Theorems 12, 13, 14 bearing in mind that c in Theorem 13 and s in Theorem 14 can be as large as $2\sqrt{q}$ or $\sqrt{q}$, respectively. The approximations are seen to be quite sharp.

The problem of evaluating $\Pi \eta_k$ as q varies with f, rather than e, held fixed requires very different methods from those of Theorems 12, 13, and 14. We treat this problem in [11].

REFERENCES

1. L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp., **21** (1967), 204–219.

2. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., **57** (1935), 391–424.

3. ———, *Linear Groups*, Dover 1958.

4. J. B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arithmetica, **11** (1965/6), 263–279.

5. J. B. Muskat and A. L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. **17** (1970), 185–216.

6. A. R. Rajwade, *The period equation for primes p congruent to* 1 (Mod 5), Proc. Camb. Phil. Soc., **69** (1971), 153–155.

7. T. Storer, *Cyclotomy and Difference Sets*, Markham 1967.

8. A. L. Whiteman, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc., **86** (1957), 401–413.

9. ———, *The cyclotomic numbers of order ten*, Proc. Symp. Appl. Math., **10**, 95–111.

10. ———, *The cyclotomic numbers of order twelve*, Acta Arith., **6** (1960), 53–76.

11. G. Myerson, A combinatorial problem in finite fields, II, to appear in Quarterly J. Math.

Received April 1, 1978.

SUNY
BUFFALO, NY 14214