A note on exponential sums*)

L. CARLITZ in Durham (N. C., U. S. A.)

To Professor L. Rédei on his sixtieth birthday

1. Let p be an odd prime and let ζ denote a primitive p-th root of 1. Put

$$B=\sum_{s=1}^{p-1}c_s\zeta^s \qquad (c_s=\pm 1), \tag{1.1}$$

where the coefficients c_s independently take on the values ± 1. The number of sums B is evidently 2^{p-1}. Also put

$$B_r=\sum_{s=1}^{r}c_s\zeta^{k_s} \qquad (c_s=\pm 1), \tag{1.2}$$

where $r\leqq p-1$ and

$$1\leqq k_1<k_2<\cdots<k_r\leqq p-1.$$

RÉDEI [1, Theorems 6, 7] has proved the following results.

Theorem *A. The sum B satisfies*

$$(1-\zeta)^{\frac{1}{2}(p-1)}\,\Big|\,B \tag{1.3}$$

if and only if

$$B=\pm\sum_{s=1}^{p-1}\left(\frac{s}{p}\right)\zeta^s; \tag{1.4}$$

that is, if and only if B is a Gauss sum. If (1.3) *does not hold, then B is divisible by at most* $(1-\zeta)^{\frac{1}{4}(p-1)}$*; this will occur if and only if* $p=4m+1$ *and*

$$B=\pm(\eta_0-\eta_2)\pm(\eta_1-\eta_3),$$

where g is a primitive root (mod p) *and*

$$\eta_j=\sum_{s=0}^{m-1}\zeta^{g^{4s+j}} \qquad (j=0,1,2,3).$$

*) Research prepared under National Science Foundation grant NSF—G 9425.

Theorem *B*. *If* B_r *satisfies*

$$(1-\zeta)^e \mid B_r, \tag{1.5}$$

then $e \leqq \frac{1}{2}r$.

The proof of these results depend upon some theorems concerning lacunary polynomials in the finite field $GF(p)$.

It may be of interest to note some corollaries of RÉDEI's theorems. If B is defined by (1.1) we may ask when B satisfies

$$|B|^2 = p. \tag{1.6}$$

Since

$$|B|^2 = B\bar{B}, \qquad \bar{B} = \sum_{s=1}^{p-1} c_s \zeta^{-s},$$

it is evident that $|B|^2$ is an integer of the cyclotomic field $R(\zeta)$, where R denotes the rational field. Hence, in place of (1.6), we may ask when B satisfies the weaker condition

$$|B|^2 \equiv 0 \pmod{p}. \tag{1.7}$$

Since $\mathfrak{p} = (1-\zeta)$ is a prime ideal of $R(\zeta)$ such that $(p) = \mathfrak{p}^{p-1}$, (1.7) is equivalent to

$$B\bar{B} \equiv 0 \quad (\mathfrak{p}^{p-1}). \tag{1.8}$$

Now suppose that

$$\mathfrak{p}^e \mid B, \qquad \mathfrak{p}^{e+1} \nmid B; \tag{1.9}$$

applying the automorphism $\zeta \to \zeta^{-1}$, it is clear that (1.9) implies

$$\mathfrak{p}^e \mid \bar{B}, \qquad \mathfrak{p}^{e+1} \nmid \bar{B}.$$

It follows that

$$\mathfrak{p}^{2e} \mid B\bar{B}, \qquad \mathfrak{p}^{2e+1} \nmid B\bar{B}. \tag{1.10}$$

Comparing (1.10) with (1.8), we infer that

$$2e \geqq p-1. \tag{1.11}$$

Thus (1.8) implies (1.3) and therefore by the first of RÉDEI's results quoted above it follows that (1.4) holds. We may accordingly state

Theorem 1. *The sum B satisfies* (1.7) *if and only if* (1.4) *holds, that is if and only if B is a Gauss sum.*

As an immediate corollary, we have

Theorem 2. *The sum B satisfies* (1.6) *if and only is B if a Gauss sum.*

2. If we use the fuller notation

$$B(\zeta^k)=\sum_{s=1}^{p-1} c_s\zeta^{sk} \qquad (1\leqq k\leqq p-1), \tag{2.1}$$

where, as above, $c_s=\pm 1$, then we have

$$\sum_{k=1}^{p-1}|B(\zeta^k)|^2=\sum_{k=1}^{p-1}\sum_{s=1}^{p-1}c_s\zeta^{sk}\sum_{t=1}^{p-1}c_t\zeta^{-tk}=\sum_{s,\,t=1}^{p-1}c_sc_t\sum_{k=1}^{p-1}\zeta^{(s-t)k}.$$

We shall assume that the c_s satisfy the condition

$$\sum_{s=1}^{p-1}c_s=0. \tag{2.2}$$

Then it is clear from the above that

$$\sum_{k=1}^{p-1}|B(\zeta^k)|^2=\sum_{s,\,t=1}^{p-1}c_sc_t\sum_{k=0}^{p-1}\zeta^{(s-t)k}=p\sum_{s=1}^{p-1}c_s^2,$$

so that

$$\sum_{k=1}^{p-1}|B(\zeta^k)|^2=p(p-1). \tag{2.3}$$

According to (2.3), the number $|B(\zeta^k)|^2$ is on the average equal to p. In view of the restriction (2.2), the number of sums $B(\zeta^k)$, for fixed ζ^k, is $\binom{p-1}{m}$, where $p=2m+1$; by Theorem 2, only two of the sums satisfy (1.6). Hence if $B(\zeta^k)$ is not a Gauss sum but (2.2) is satisfied, it follows from (2.3) that both inequalities

$$|B(\zeta^k)|^2>p, \qquad |B(\zeta^k)|^2<p$$

are satisfied for appropriate values of k. This suggests the problem of determining upper and lower bounds for $|B(\zeta^k)|$. However for $\zeta=e^{2\pi i/p}$,

$$c_1=\cdots=c_m=1, \qquad c_{m+1}=\cdots=c_{2m}=-1, \tag{2.4}$$

where $p=2m+1$, we have

$$B=B(\zeta)=\sum_{s=1}^{m}\zeta^s-\sum_{s=m+1}^{2m}\zeta^s=\zeta(1-\zeta^m)\sum_{s=0}^{m-1}\zeta^s=\frac{\zeta(1-\zeta^m)^2}{1-\zeta},$$

so that

$$|B|=\left|\frac{(1-\zeta^m)^2}{1-\zeta}\right|=2\,\frac{\sin^2\dfrac{m\pi}{p}}{\sin\dfrac{\pi}{p}}.$$

Therefore for large p we get

$$|B| \sim \frac{2}{\pi} p.$$

In particular, the statement

(2.6) $$B = o(p)$$

for all B satisfying (2.2), is false.

Again for the choice

(2.7) $$c_1 = c_3 = \cdots = c_{2m-1} = 1, \qquad c_2 = c_4 = \cdots = c_{2m} = -1,$$

we have

$$B = B(\zeta) = \sum_{s=1}^{2m} (-1)^{s-1} \zeta^s = \frac{\zeta(1-\zeta^{2m})}{1+\zeta},$$

so that

$$|B| = \left| \frac{1-\zeta^{2m}}{1+\zeta} \right| = \frac{\sin \frac{2m\pi}{p}}{\cos \frac{\pi}{p}} = \frac{\sin \frac{\pi}{p}}{\cos \frac{\pi}{p}}.$$

For large p this implies

(2.8) $$B \sim \frac{\pi}{p}.$$

Thus the statement

(2.9) $$|B| > c > 0$$

for all B satisfying (2.2) where c is independent of p, is also false. It seems plausible that

(2.10) $$\frac{\pi}{p} < |B| < \frac{2p}{\pi}$$

for all B satisfying (2.2).

3. Turning now to B_r defined by (1.2) we may apply the argument used in the proof of Theorem 1 together with Theorem *A* of RÉDEI to prove the following result.

Theorem 3. *If $r < p-1$, the congruence*

(3.1) $$|B_r|^2 \equiv 0 \pmod{p}$$

holds for no

$$B_r = \sum_{s=1}^{r} c_s \zeta^{k_s} \qquad (c_s = \pm 1),$$

where $1 \leqq k_1 < k_2 < \cdots < k_r < p-1$. A fortiori the equality

(3.2) $$|B_r|^2 = p$$

holds for no B_r.

If we put

$$B_r(\zeta^h) = \sum_{s=1}^{r} c_s \zeta^{k_s h} \qquad (1 \leqq h \leqq p-1), \tag{3.3}$$

and in addition assume that

$$\sum_{s=1}^{r} c_s = 0, \tag{3.4}$$

then exactly as in the proof of (2.3), we have

$$\sum_{h=1}^{p-1} |B_r(\zeta^h)|^2 = pr. \tag{3.5}$$

Thus, when (3.4) is satisfied, $|B_r(\zeta^h)|^2$ is on the average equal to $pr/(p-1)$; for large p, the average is therefore r.

Clearly (3.4) requires that r be even. Put $r=2t$, $\zeta = e^{2\pi i/p}$, $p=2m+1$, and consider

$$B_r = \sum_{s=1}^{t} \zeta^s = \sum_{s=m+1}^{m+t} \zeta^s = \frac{\zeta(1-\zeta^m)(1-\zeta^t)}{1-\zeta}. \tag{3.6}$$

Then

$$|B_r| = \frac{2 \sin \frac{m\pi}{p} \sin \frac{t}{p}}{\sin \frac{\pi}{p}}.$$

For large p it follows that

$$|B_r| \sim \frac{2p}{\pi} \sin \frac{t\pi}{p}. \tag{3.7}$$

In particular if $r = o(p)$, (3.7) yields

$$|B_r| \sim r. \tag{3.8}$$

In the next place, if we take

$$B_r = \sum_{s=1}^{r} (-1)^{s-1} \zeta^s = \frac{\zeta(1-\zeta^r)}{1+\zeta}, \tag{3.9}$$

then

$$|B_r| = \frac{\sin \frac{t\pi}{p}}{\cos \frac{\pi}{p}},$$

so that for large p it follows that

$$|B_r| \sim \sin \frac{t\pi}{p}. \tag{3.10}$$

In particular if $r=o(p)$, (3.10) becomes

$$|B_r| \sim \frac{r\pi}{2p}. \tag{3.11}$$

4. We now give another proof of RÉDEI's theorem that (1.3) holds only when B is a Gauss sum. In the first place (1.3) is equivalent to

$$\sum_{s=1}^{p-1} s^j c_s \equiv 0 \pmod{p} \qquad \left(1 \leqq j < \frac{1}{2}(p-1)\right). \tag{4.1}$$

This is essentially the Lemma on p. 287 of [1]. Indeed, (4.1) follows easily from the identity

$$B = \sum_{s=1}^{p-1} c_s \zeta^s = \sum_{s=1}^{p-1} c_s (1+(\zeta-1))^s = \sum_{j=0}^{p-1} (\zeta-1)^j \sum_{s=j}^{p-1} \binom{s}{j} c_j.$$

Now consider the polynomial $f(x)$ with coefficients in the $GF(p)$ such that

$$f(0)=0, \quad f(s)=c_s \qquad (s=1,\ldots,p-1).$$

Clearly

$$f(x) = -\sum_{s=1}^{p-1} c_s \frac{x^p-x}{x-s} = -\sum_{s=1}^{p-1} c_s (x-s)^{p-1}.$$

It follows from (4.1) that

$$\deg f(x) \leqq m = \frac{1}{2}(p-1). \tag{4.2}$$

Since

$$f^2(0)=0, \quad f^2(s)=1 \qquad (s=1,\ldots,p-1),$$

it follows at once that

$$f^2(x) = x^{p-1}; \tag{4.3}$$

in view of (4.2), it is clear that (4.3) is an identity (and not merely a congruence mod (x^p-x)). Now put

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \qquad (a_j \in GF(p));$$

making use of (4.3) we get

$$f(x) = \pm x^m = \pm\left(\frac{x}{p}\right).$$

This evidently completes the proof of the theorem.

To prove the second half of Theorem A we require a little more. Suppose that B satisfies

$$\mathfrak{p}^t | B, \qquad \mathfrak{p}^{t+1} \nmid B \tag{4.4}$$

for some t in the range $1 \leqq t \leqq m$. As above we define the polynomial $f(x)$ such that

$$f(0)=0, \quad f(s)=c_s \qquad (s=1,\ldots,p-1).$$

Now (4.4) is equivalent to

$$\sum_{s=1}^{p-1} s^j c_s \begin{cases} \equiv 0 \pmod p & (1 \leqq j < t) \\ \not\equiv 0 \pmod p & (j=t); \end{cases} \tag{4.5}$$

it follows that

$$\deg f(x) = p-1-t. \tag{4.6}$$

Put

$$U(x)=\prod_{c_s=1}(x-s), \qquad V(x)=\prod_{c_s=-1}(x-s),$$

so that

$$x^{2m}-1 = U(x)V(x), \qquad \deg U(x) = \deg V(x) = m. \tag{4.7}$$

Thus $f(x)$ is uniquely determined by

$$\begin{cases} f(x) \equiv 1 \pmod{U(x)}, \\ f(x) \equiv -1 \pmod{V(x)}, \\ f(x) \equiv 0 \pmod{x}. \end{cases} \tag{4.8}$$

It is easily verified that the system (4.8) has the solution

$$f(x) = x(U(x)V'(x)-U'(x)V(x)). \tag{4.9}$$

In the next place, it follows from (4.5) and (4.7) that

$$U(x)=x^m+a_1x^{m-1}+\cdots+a_m, \qquad V(x)=x_m+b_1x^{m-1}+\cdots+b_m, \tag{4.10}$$

where $b_t=-a_t \neq 0$. Substituting in (4.9) we get

$$f(x) = 2ta_tx^{2m-t}+\ldots,$$

so that

$$\deg f(x) = 2m-t. \tag{4.11}$$

Now assume that

$$\frac{1}{2}m < t < m. \tag{4.12}$$

Using (4.7) and (4.10) we get, since $2m-2t<m$,

$$b_j = -a_j \qquad (t \leqq j \leqq m).$$

However, the coefficient of x^{2m-2t} in $U(x)V(x)$ is equal to $-a_t^2 \neq 0$. Thus (4.12) is not possible. Consequently, when $t<m$, we must have $t \leqq \frac{1}{2}m$.

For $t=\frac{1}{2}m$, the coefficient of x^{m-1} in $U(x)V(x)$ is

$$-2a_ta_{t+1}=0,$$

so that $a_{t+1}=0$. Similarly we find that

$$a_j=0 \qquad (t<j<m).$$

Thus (4.7) becomes

$$(x^{2m}-1)=(x^m+a_tx^t+a_m)(x^m-a_tx^t+b_m),$$

where

$$a_m+b_m=a_t^2, \qquad a_mb_m=-1, \qquad a_m=b_m.$$

Put $a_m=\sigma$, where $\sigma^2=-1$, then

$$a_t^2=2\sigma=(\sigma+1)^2,$$

so that $a_t=\sigma+1$. Hence we have

$$A(x)=x^m+(\sigma+1)x^t+\sigma=(x^t+1)(x^t+\sigma),$$
$$B(x)=x^m-(\sigma+1)x^t+\sigma=(x^t-1)(x^t-\sigma).$$

The second half of Theorem *A* now follows immediately.

We have incidentally proved the following result.

Theorem 4. *The sum B satisfies* (4.4) *for some t in the range* $1\leqq t\leqq m$ *if and only if there exists a factorization*

$$x^{2m}-1=(x^m+a_tx^{m-t}+\cdots+a_m)(x^m+b_tx^{m-t}+\cdots+b_t), \tag{4.13}$$

where $a_tb_t\neq 0$.

For $t=m$ or $\frac{1}{2}m$ the possible factorizations (4.13) are described by Theorems 1 and 2 of RÉDEI's paper. It is easy to show that when $t|m$ such factorizations exist. Indeed, if $m=tk$, k odd, we have

$$x^m-1=(x^t-1)(x^{(k-1)t}+x^{(k-2)t}+\cdots+1),$$
$$x^m+1=(x^t+1)(x^{(k-1)t}-x^{(k-2)t}+\cdots+1)$$

and we get the factors

$$U=x^m-2x^{m-t}+\cdots-1, \qquad V=x^m+2x^{m-t}+\cdots+1.$$

For k even, let σ be an integer such that $\sigma^k=-1$; then

$$x^m+1=x^{tk}-\sigma^k=(x^t-\sigma)(x^{(k-1)t}+\sigma x^{(k-2)t}+\cdots+\sigma^{k-1})$$

and we get the factors

$$U=x^m+(\sigma-1)x^{m-t}+\cdots+\sigma^{k-1}, \qquad V=x^m-(\sigma-1)x^{m-t}+\cdots+\sigma.$$

However the condition $t|m$ is not necessary. For example when $p=17$, $t=3$, a possible factor is

$$x^8-x^5+4x^3-8x^2+8x-4=$$
$$(x-1)(x+2)(x+3)(x-4)(x+5)(x-6)(x-7)(x+8).$$

For $p=19$, $t=4$, a factorization (4. 13) is apparently not possible. Assume that

$$x^{18}-1=(x^9-x^5+ax^4+bx^3+cx^2+dx+e)\cdot$$
$$\cdot(x^9+x^5+a'x^4+b'x^3+c'x^2+d'x+e');$$

there is no loss in generalization in normalizing the coefficient of x^5. We find first that

$$a'=-a, \qquad b'=-b, \qquad c'=-c.$$

Also we get the conditions

$$a^2=2b, \qquad ab=c, \qquad -2bc-(e'-e)+a(d'-d)=0,$$
$$-c^2+a(e'-e)+b(d'-d)=0, \qquad b(e'-e)+c(d'-d)=0.$$

Now the last three equations imply

$$\begin{vmatrix} -2bc & -1 & a \\ -c^2 & a & b \\ 0 & b & c \end{vmatrix}=c(2b^3-c^2-3abc)=0.$$

Since $abc\neq 0$, we get, using $ab=c$,

$$b^3=2c^2.$$

But $a^2=2b$, $ab=c$ imply $c^2=2b^3$, so that we have a contradiction.

Thus the question remains open what values of t is the range $1\leqq t<\frac{1}{2}m$ can satisfy (4. 4).

Reference

[1] L. Rédei, Zwei Lückensätze über Polynome in endlichen Primkörpern mit Anwendung auf die endlichen Abelschen Gruppen und die Gaußischen Summen, *Acta Math.*, **79** (1947), 273—290.

(Received September 7, 1959)