COLLOQUIUM MATHEMATICUM

VOL. XX 1969 FASC. 1

SUMS OF POWERS OF GENERATORS OF A FINITE FIELD

BY

K. SZYMICZEK (KATOWICE)

1. Let $\mathscr{F} = \mathscr{F}_q$ be a finite field of $q = p^n$ elements. It is well-known that the multiplicative group $\mathscr{F}^*$ of the field $\mathscr{F}$ is a cyclic group of order $q-1$ and has $\varphi(q-1)$ generators (cf. [1], chapter V). In this paper we are concerned with sums of powers of generators of the field $\mathscr{F}$ and with some related sums. The first result is the following

THEOREM I. *If g runs through all generators of a finite field $\mathscr{F}_q$ and m is an integer, then*

$$\sum g^m = \mu(e)\frac{\varphi(q-1)}{\varphi(e)}, \quad \textit{where } e = \frac{q-1}{(m, q-1)},$$

μ and φ denote the Möbius and the Euler functions, respectively and the integer on the right has to be multiplied by the unity of $\mathscr{F}_q$.

This theorem is a generalization of a result of Gauss ([4], Art. 81), who proved that the sum of primitive roots of a prime p is congruent to $\mu(p-1)$ modulo p (the case of $\mathscr{F} = Z_p$ = the field of integers mod p, and $m = 1$). In the case when $\mathscr{F} = Z_p$ and m is a positive integer, we get from Theorem I Forsyth's [3] theorem on sums of powers of primitive roots of a prime p. Other proofs of that theorem were given by Czarnota [2] and Szymiczek [7].

The mentioned theorem of Gauss was generalized by Stern [6], who established a similar congruence property for the sum of numbers belonging to any divisor of $p-1$ modulo p. Moller [5] found a congruence for the sum of m-th powers of numbers belonging to any divisor of $p-1$ modulo p (see also Zuckerman [8] for a simpler proof).

All above-mentioned results are special cases of the following

THEOREM II. *Let e be a divisor of $q-1$. If h runs through all elements of the field $\mathscr{F}$ whose order in the group $\mathscr{F}^*$ is e, and m is an integer, then*

$$(1) \qquad \sum_{\operatorname{ord} h = e} h^m = \mu(e_1)\frac{\varphi(e)}{\varphi(e_1)},$$

where $e_1 = e/(m, e)$.

We also state the following theorem:

THEOREM III. *Let x be a divisor of $q-1$. The sum of the m-th powers of all elements of $\mathscr{F}_q$ whose orders in $\mathscr{F}^*$ are divisors of x, is equal to x or zero, according as m is or is not a multiple of x.*

The proof of theorem III, given by Zuckerman [8] for the special case of $\mathscr{F} = Z_p$, may be easily extended to the general case. Theorem III covers the results of Moller ([5], Th. II) and Zuckerman [8], and it is a generalization of a well-known theorem on the sum of the m-th powers of all the numbers $1, \dots, p-1$ modulo p (the case of $\mathscr{F} = Z_p$ and $x = p-1$).

Now, let F be an algebraic number field and R the ring of all integers in F. Let $\mathfrak{p}$ be a prime ideal in R and $N(\mathfrak{p}) = p^f$. Then the ring $R/\mathfrak{p}$ is a finite field of p^f elements. If the class $[a]$, $a \in R$, is a generator of the multiplicative group of the field $R/\mathfrak{p}$, then a is a primitive root $\bmod \mathfrak{p}$. Of course, $a \in R$ is a primitive root $\bmod \mathfrak{p}$ if and only if $t = N(\mathfrak{p})-1$ is the smallest positive exponent satisfying $a^t \equiv 1 \pmod{\mathfrak{p}}$. Now, from theorems I, II and III we derive

THEOREM IV. (1) *If a runs through all non-congruent primitive roots modulo $\mathfrak{p}$ and m is an integer, then*

$$\sum a^m \equiv \mu(e)\frac{\varphi(p^f-1)}{\varphi(e)} \pmod{\mathfrak{p}}, \quad \textit{where } e = \frac{p^f-1}{(m, p^f-1)}$$

and $p^f = N(\mathfrak{p})$.

(2) *Let e be a divisor of p^f-1. If β runs through all non-congruent numbers belonging to the exponent e modulo $\mathfrak{p}$ and m is an integer, then*

$$\sum \beta^m \equiv \mu(e_1)\frac{\varphi(e)}{\varphi(e_1)} \pmod{\mathfrak{p}}, \quad \textit{where } e_1 = \frac{e}{(m, e)}.$$

(3) *Let x be a divisor of p^f-1. The sum of the m-th powers of all numbers belonging modulo $\mathfrak{p}$ to any of the divisors of x, is congruent modulo $\mathfrak{p}$ to x or zero, according as m is or is not a multiple of x.*

(4) *If γ runs through a complete system of residues modulo $\mathfrak{p}$ and m is an integer, then*

$$\sum \gamma^m \equiv 0 \quad \textit{or} \quad p^f-1 \pmod{\mathfrak{p}},$$

according as m is or is not a multiple of p^f-1.

2. Now we prove Theorem II. Consider the sum

$$S = \sum_{\operatorname{ord} h = e} h^m.$$

It contains $\varphi(e)$ terms and each of them is an element of order $e_1 = e/(m, e)$ in $\mathscr{F}^*$. We prove here the two following statements:

I. Each of the $\varphi(e_1)$ elements of the group $\mathscr{F}^*$, whose order is e_1, occurs in the sum S exactly $\varphi(e)/\varphi(e_1)$ times.

II. $S_1 = \mu(e_1)$.

From I it follows that

$$S = \frac{\varphi(e)}{\varphi(e_1)} S_1, \tag{2}$$

where S_1 is the sum of all elements of the group $\mathscr{F}^*$, whose order is e_1:

$$S_1 = \sum_{\operatorname{ord} h = e_1} h.$$

Relation (1) follows now at once from (2) and II.

The proof of statement I depends of the following lemma (cf. [7]):

LEMMA 1. *Suppose that* $M = NK$, $1 < N < M$, *and that* $a_1, \ldots, a_{\varphi(M)}$ *is a complete set of residues prime to* M. *If* $b_i \equiv a_i \pmod N$, $0 < b_i < N$, $i = 1, \ldots, \varphi(M)$, *then each of the numbers less than and prime to* N *occurs among the numbers* b_i *with the same frequency* $\varphi(M)/\varphi(N)$.

Proof. Let $K = PR$ and $N = \bar{P}Q$, where $(Q, R) = 1$ and P and $\bar{P}$ have the same prime factors (in the case of $(N, K) = 1$, we have $P = \bar{P} = 1$). Suppose that b is an integer satisfying $(b, N) = 1$ and $0 < b < N$. Hence, each of the numbers $b, b+N, \ldots, b+(K-1)N$ is prime to N, and thus $b+xN$ is prime to M if and only if it is prime to R. The numbers $b+xN$, $x = 0, 1, \ldots, K-1$ form P complete sets of residues modulo R:

$$\begin{array}{lll} b, & b+N, & \ldots, b+(R-1)N, \\ b+RN, & b+(R+1)N, & \ldots, b+(2R-1)N, \\ \cdots & \cdots & \cdots \\ b+(P-1)RN, & b+[(P-1)R+1]N, & \ldots, b+(PR-1)N. \end{array}$$

In fact, each row contains R distinct numbers and two numbers belonging to the s-th row are congruent modulo R if and only if they are equal; namely, if $0 \leqslant i < j \leqslant R-1$ and $b+(sR+i)N \equiv b+(sR+j)N \pmod R$, then, because of $(R, N) = 1$, we have $i \equiv j \pmod R$, and so $i = j$. Each of the P complete sets of residues mod R contains exactly $\varphi(R)$ of numbers prime to R, i.e., $P\varphi(R)$ of the numbers $b+xN$, $x = 0, 1, \ldots$ $\ldots, K-1$ are prime to R, and so $P\varphi(R)$ of the numbers $b+xN$ are prime to M.

On the other hand, it is easy to verify that $P\varphi(R) = \varphi(M)/\varphi(N)$. Thus, among the numbers congruent to $b \pmod N$ and less than M there are $\varphi(M)/\varphi(N)$ numbers prime to M and the lemma is proved.

Now we prove statement I. Let h_1 be a fixed element of the group $\mathscr{F}^*$ of order e. Hence, if $h \in \mathscr{F}^*$ and ord $h = e$, then $h = h_1^a$, where $(a, e) = 1$. Suppose that $a_1, \ldots, a_{\varphi(e)}$ is a complete set of residues prime to e. Then we have

$$S = \sum_{\operatorname{ord} h = e} h^m = \sum_{i=1}^{\varphi(e)} h_1^{ma_i}.$$

In the last sum two terms, $h_1^{ma_i}$ and $h_1^{ma_j}$, are equal if and only if $ma_i \equiv ma_j \pmod{e}$, i.e., if and only if $a_i \equiv a_j \pmod{e_1}$. Putting $M = e$, $N = e_1$ in Lemma 1 we see that the set $a_1, \ldots, a_{\varphi(e)}$ falls into $\varphi(e)/\varphi(e_1)$ complete sets of residues prime to e_1 and thus

$$S = \frac{\varphi(e)}{\varphi(e_1)} \sum_{i=1}^{\varphi(e_1)} h_1^{mb_i},$$

where $b_1, \ldots, b_{\varphi(e_1)}$ is a complete set of residues prime to e_1. This proves statement I. In the last sum each element of order e_1 is represented, and so (2) follows.

LEMMA 2. *If h runs through all elements of order e (in $\mathscr{F}^*$), then* $S_e = \sum h = \mu(e)$.

Proof. Consider first the case $e = r$, r being a prime. If ord $h = r$, then all elements of order r in $\mathscr{F}^*$ are h^a, $a = 1, 2, \ldots, r-1$, and so

$$S_e = h + h^2 + \ldots + h^{r-1} = -1 = \mu(e).$$

Now, put $e = r^t$, $t > 1$, where r is a prime. If ord $h = r^t$, then all elements of order r^t in $\mathscr{F}^*$ are of the form h^a, where $(a, r^t) = 1$, $1 \leqslant a < r^t$. Thus

$$\begin{aligned} S_e &= h + h^2 + \ldots + h^{r^t-1} - (h^r + h^{2r} + \ldots + h^{(r^t-1)r}) \\ &= \frac{h^{r^t}-1}{h-1} - 1 - \left(\frac{h^{r^t}-1}{h^r-1} - 1\right) = 0 = \mu(e). \end{aligned}$$

Thus lemma 2 is proved in the case when e is a prime or a prime power. Next, we prove that the sum S_e is multiplicative, i.e., if $(e_1, e_2) = 1$, then $S_{e_1e_2} = S_{e_1}S_{e_2}$. Let ord $h_i = e_i$, $i = 1, 2$, $(e_1, e_2) = 1$. We then have ord $h_1h_2 = e_1e_2$. On the other hand, if ord $h_i' = e_i$, $i = 1, 2$ and $h_1h_2 = h_1'h_2'$, then $h_1 = h_1'$, $h_2 = h_2'$. In fact, $(h_1h_2)^{e_2} = (h_1'h_2')^{e_2}$, whence $h_1^{e_2} = h_1'^{e_2}$. Moreover, $h_1' = h_1^s$ and $(s, e_1) = 1$, and we have $h_1^{e_2} = h_1^{se_2}$, $e_2 \equiv se_2 \pmod{e_1}$, $s \equiv 1 \pmod{e_1}$, $h_1' = h_1$ and $h_2' = h_2$. Thus the representation of an element of order e_1e_2 as a product of two elements of orders e_1 and e_2, respectively, is unique. If, now, $r_1, \ldots, r_{\varphi(e_1)}$ is a complete set of residues prime to e_1, and $s_1, \ldots, s_{\varphi(e_2)}$ a complete set of residues prime to e_2, then

$$S_{e_1}S_{e_2} = \sum h_1^{r_i} \sum h_2^{s_j} = \sum h_1^{r_i} h_2^{s_j} = S_{e_1e_2}.$$

To prove lemma 2, we put $e = \prod e_i$, where e_i are prime powers, and apply the multiplicative property of S_e:

$$S_e = \prod S_{e_i} = \prod \mu(e_i) = \mu(e).$$

Lemma 2 is identical with statement II, and so the proof of theorem II is complete.

REFERENCES

[1] A. A. Albert, *Fundamental concepts of higher algebra*, Chicago 1956.

[2] A. Czarnota, *Kongruencje spelniane przez sumy potęg pierwiastków pierwotnych względem modulu pierwszego*, Roczniki PTM, Seria I: Prace Matematyczne 8 (1964), p. 131-142.

[3] A. R. Forsyth, *Primitive roots of prime numbers and their residues*, Messenger of Mathematics 13 (1883/4), p. 180-185.

[4] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig 1801.

[5] R. Moller, *Sums of powers of numbers having a given exponent modulo a prime*, American Mathematical Monthly 59 (1952), p. 226-229.

[6] M. A. Stern, *Bemerkungen über höhere Arithmetik*, Journal für Mathematik 6 (1830), p. 147-153.

[7] K. Szymiczek, *Two proofs of the Forsyth-Czarnota theorem*, Zeszyty Naukowe Wyższej Szkoły Pedagogicznej w Katowicach, Sekcja Matematyki, 6 (1968), p. 49-53.

[8] H. S. Zuckerman, *Additional remarks to the paper of Moller*, American Mathematical Monthly 59 (1952), p. 229-230.

SILESIA UNIVERSITY, KATOWICE

Reçu par la Rédaction le 24. 2. 1968