MATHEMATICAL NOTES

EDITED BY DAVID DRASIN

Manuscripts for this Department should be sent to David Drasin, Division of Mathematical Sciences. Purdue University, Lafayette, IN 47907.

ON A RESULT OF LIBRI AND LEBESGUE

K. S. WILLIAMS, Carleton University, Ottawa

1. Introduction. In this note we observe how a simple property of a primitive nth root of unity provides us with a counting function for the number of solutions of a congruence $f(x_1, \cdots, x_k) \equiv 0 \pmod{n}$. We illustrate the idea by taking $f(x_1, \cdots, x_k) = x_1^l + \cdots + x_k^l$ and a prime $n = p \equiv 1 \pmod{l}$. We are led naturally to the q-nomial periods of the pth roots of unity where $q = (p-1)/l$ [2]. We express the number of solutions of $x_1^l + \cdots + x_k^l \equiv 0 \pmod{p}$ in terms of these periods, rediscovering an old result due to Libri and Lebesgue [1]. An alternative form of this result is also proved which provides a generalization of one due to the author when $l = 3$ (see [4]). The formula of Libri and Lebesgue has been generalized by Weil [3]. The material in this note is not new but we hope that perhaps the presentation is.

2. Two properties of $\omega(n)$. For any integer $n \geqq 2$ let $\omega(n) = \exp(2\pi i/n)$. A well-known property possessed by $\omega(n)$ is the following:

LEMMA 1. *If m is an integer, then*

$$\sum_{r=0}^{n-1} \{\omega(n)\}^{mr} = \begin{cases} n, & \text{if } m \equiv 0 \pmod{n}, \\ 0, & \text{if } m \not\equiv 0 \pmod{n}. \end{cases}$$

Proof. The left-hand side is just a geometric progression.

This property of $\omega(n)$ guarantees that any complex-valued function $f(m)$ (m an integer) which is periodic with period n has a finite Fourier series.

LEMMA 2. *If $f(m)$ is periodic in m with period n, then*

$$f(m) = \sum_{r=0}^{n-1} a(r)\{\omega(n)\}^{mr},$$

where $a(r) = (1/n)\sum_{s=0}^{n-1} f(s)\{\omega(n)\}^{-rs}$.

Proof. We have, using Lemma 1,

$$\sum_{r=0}^{n-1} a(r)\{\omega(n)\}^{mr} = \frac{1}{n}\sum_{r=0}^{n-1}\sum_{s=0}^{n-1} f(s)\{\omega(n)\}^{(m-s)r}$$

$$= \frac{1}{n}\sum_{s=0}^{n-1} f(s)\sum_{r=0}^{n-1}\{\omega(n)\}^{(m-s)r} = f(m).$$

3. Counting function. Lemma 1 provides us with a counting function for congruences modulo n, for if $f(x_1, \cdots, x_k)$ is a polynomial with integral coefficients, then the number of solutions $(x_1, \cdots, x_k)$ of $f(x_1, \cdots, x_k) \equiv 0 \pmod{n}$ satisfying $0 \leqq x_i < n$ is given by

$$\sum_{x_1, \cdots, x_k=0}^{n-1} \left\{ \frac{1}{n} \sum_{r=0}^{n-1} \{\omega(n)\}^{f(x_1, \cdots, x_k)r} \right\} = \frac{1}{n} \sum_{r=0}^{n-1} \sum_{x_1, \cdots, x_k=0}^{n-1} \{\omega(n)\}^{rf(x_1, \cdots, x_k)}.$$

This can be simplified if $f(x_1, \cdots, x_k)$ is separable in the variables $x_1, \cdots, x_k$. We consider an application where this is so.

4. Application to $x_1^l + \cdots + x_k^l$. We take $f(x_1, \cdots, x_k) = x_1^l + \cdots + x_k^l$ and a prime $n = p \equiv 1 \pmod{l}$, and use the law of exponents: $\omega^{a+b} = \omega^a \omega^b$. Then the number $N_p(l, k)$ of solutions $(x_1, \cdots, x_k)$ of $x_1^l + \cdots + x_k^l \equiv 0 \pmod{p}$ is given by

$$\begin{aligned} N_p(l, k) &= \frac{1}{p} \sum_{r=0}^{p-1} \sum_{x_1, \cdots, x_k=0}^{p-1} \{\omega(p)\}^{r(x_1^l + \cdots + x_k^l)} \\ &= \frac{1}{p} \sum_{r=0}^{p-1} \left\{ \sum_{x=0}^{p-1} \{\omega(p)\}^{rx^l} \right\}^k. \end{aligned}$$

Let us write $S_p(l, r) = \sum_{x=0}^{p-1} \{\omega(p)\}^{rx^l}$. We note that $S_p(l, r)$ is periodic in r with period p, and

$$S_p(l, 0) = \sum_{x=0}^{p-1} 1 = p,$$

so that $pN_p(l, k) - p^k = \sum_{r=1}^{p-1} \{S_p(l, r)\}^k$. In the summation, r takes on the values $1, 2, \cdots, p-1$. These are $g^0, g^1, g^2, \cdots, g^{p-2}$ (taken modulo p) in some order, where g is a primitive root modulo p. As $S_p(l, r)$ is periodic with period p, we have

$$pN_p(l, k) - p^k = \sum_{s=0}^{p-2} \{S_p(l, g^s)\}^k. \tag{4.1}$$

We next show that $S_p(l, g^s)$ is periodic in s with period l.

LEMMA 3. *For all integers* s, $S_p(l, g^s) = S_p(l, g^{s+l})$.

Proof. We have

$$S_p(l, g^{s+l}) = \sum_{x=0}^{p-1} \{\omega(p)\}^{x^l g^{s+l}} = \sum_{x=0}^{p-1} \{\omega(p)\}^{(gx)^l g^s}.$$

Now the mapping $x \to g^{-1}x$ (so that $gx \to x$) taken modulo p is a bijection on $\{0, 1, \cdots, p-1\}$, so that

$$\sum_{x=0}^{p-1} \{\omega(p)\}^{(gx)^l g^s} = \sum_{x=0}^{p-1} \{\omega(p)\}^{x^l g^s},$$

that is, $S_p(l, g^{s+l}) = S_p(l, g^s)$ as required.

As $p-1 \equiv 0 \pmod{l}$ this periodicity implies

$$\sum_{s=0}^{p-2} \{S_p(l, g^s)\}^k = q \sum_{s=0}^{l-1} \{S_p(l, g^s)\}^k,$$

so that (4.1) becomes

$$pN_p(k, l) - p^k = q \sum_{s=0}^{l-1} \{S_p(l, g^s)\}^k.$$

Now let us examine $S_p(l, g^s)$ (for $s=0, 1, \cdots, l-1$). We have

$$S_p(l, g^s) = \sum_{x=0}^{p-1} \{\omega(p)\}^{g^s x^l} = 1 + \sum_{x=1}^{p-1} \{\omega(p)\}^{g^s x^l}$$
$$= 1 + \sum_{t=0}^{p-2} \{\omega(p)\}^{g^{s+lt}} = 1 + \sum_{r=0}^{l-1} \sum_{u=0}^{q-1} \{\omega(p)\}^{g^{s+l(qr+u)}}.$$

But $g^{p-1} \equiv 1$, so we have

$$S_p(l, g^s) = 1 + \sum_{r=0}^{l-1} \sum_{u=0}^{q-1} \{\omega(p)\}^{g^{s+lu}} = 1 + l \sum_{u=0}^{q-1} \{\omega(p)\}^{g^{s+lu}}.$$

The expressions $\sum_{u=0}^{q-1} \{\omega(p)\}^{g^{s+lu}}$ are called the *q-nomial periods* of the pth roots of unity [2]. We write

$$\eta_s = \sum_{u=0}^{q-1} \{\omega(p)\}^{g^{s+lu}}$$

so that we have the result of Libri and Lebesgue [1]:

THEOREM 1. *The number $N_p(k, l)$ of solutions of $x_1^l + \cdots + x_k^l \equiv 0 \pmod{p}$ is given by* $N_p(k, l) = p^{k-1} + (q/p) \sum_{s=0}^{l-1} \{1 + l\eta_s\}^k$.

5. An alternative expression for $N_p(k, l)$. We can apply Lemma 2 to $S_p(l, g^s)$ (as it is periodic in s with period l) to obtain a different expression for $S_p(l, g^s)$ and thus a different expression for $N_p(k, l)$. By Lemma 2 we have $S_p(l, g^s) = \sum_{r=0}^{l-1} a(r) \{\omega(l)\}^{rs}$, where

$$a(r) = \frac{1}{l} \sum_{s=0}^{l-1} S_p(l, g^s) \{\omega(l)\}^{-rs}$$
$$= \frac{1}{l} \sum_{s=0}^{l-1} \left\{1 + l \sum_{u=0}^{q-1} \{\omega(p)\}^{g^{s+lu}}\right\} \{\omega(l)\}^{-rs}$$
$$= \frac{1}{l} \sum_{s=0}^{l-1} \{\omega(l)\}^{-rs} + \sum_{s=0}^{l-1} \sum_{u=0}^{q-1} \{\omega(p)\}^{g^{s+lu}} \{\omega(l)\}^{-rs}$$

$$= \frac{1}{l}\sum_{s=0}^{l-1}\{\omega(l)\}^{-rs} + \sum_{t=0}^{p-2}\{\omega(p)\}^{g^t}\{\omega(l)\}^{-rs}$$

$$= \begin{cases} 1 + \sum_{t=0}^{p-2}\{\omega(p)\}^{g^t}, & r = 0, \\ 0 + \sum_{t=0}^{p-2}\{\omega(p)\}^{g^t}\{\omega(l)\}^{-rs}, & r = 1, 2, \cdots, l-1, \end{cases}$$

$$= \begin{cases} 0, & r = 0, \\ \sum_{t=0}^{p-2}\{\omega(p)\}^{g^t}\{\omega(l)\}^{-rs}, & r \not\equiv 0. \end{cases}$$

Writing $\tau_r = \sum_{t=0}^{p-2}\{\omega(p)\}^{g^t}\{\omega(l)\}^{-rs}$, where r is any integer, we have

$$S_p(l, g^s) = \sum_{r=1}^{l-1}\{\omega(l)\}^{sr}\tau_r,$$

giving the following theorem:

THEOREM 2. *The number $N_p(k, l)$ of solutions of* $x_1^l + \cdots + x_k^l \equiv 0 \pmod p$ *is given by*

$$N_p(k, l) = p^{k-1} + \frac{q}{p}\sum_{s=0}^{l-1}\left\{\sum_{r=1}^{l-1}\{\omega(l)\}^{sr}\tau_r\right\}^k.$$

This generalizes a result of the author [4] when $l=3$, viz.,

$$N_p(k, 3) = p^{k-1} + [(p-1)/3p][(\tau_1+\tau_2)^k + (\omega\tau_1+\omega^2\tau_2)^k + (\omega^2\tau_1+\omega\tau_2)^k],$$

where $\omega \equiv \omega(3) = \frac{1}{2}(-1+\sqrt{-3})$.

References

1. V. A. Lebesgue, Recherches sur les nombres, J. Math. Pures Appl., 2 (1837) 253–292.
2. G. B. Mathews, Theory of Numbers, Chelsea, New York, 1962, p. 191.
3. A. Weil, Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc., 55 (1949) 497–508.
4. K. S. Williams, On the number of solutions of a congruence, this MONTHLY, 73 (1966) 44–49.

LIMIT POINTS OF SEQUENCES IN METRIC SPACES

M. D. AŠIĆ AND D. D. ADAMOVIĆ, University of Belgrade, Yugoslavia

The aim of this paper is to generalize both statements of the following theorem [1]:

THEOREM A. *Let $C(\xi)$ be the set of limit points of the bounded complex sequence ξ. Then $C(\xi)$ is connected if and only if there exists a subsequence $\eta=(y_n)$ of ξ such that $C(\eta)=C(\xi)$ and $y_{n+1}-y_n\to 0$ $(n\to\infty)$.*