SOME ARITHMETICAL FUNCTIONS IN FINITE FIELDS

by STEPHEN D. COHEN

(Received 17 October, 1968)

1. Introduction. In this paper, we investigate various " arithmetical " functions associated with the factorisation of polynomials in $GF[q, X_1, \ldots, X_k]$, where $k \geqq 1$ and $GF[q]$ is the finite field of order q. We shall assume throughout that all polynomials discussed are non-zero and have been normalised by selecting one polynomial from each equivalence class with respect to multiplication by non-zero elements of $GF[q]$. The constant polynomial will be denoted by 1. With this normalisation, $GF[q, X_1, \ldots, X_k]$ becomes a unique factorisation domain. When $k = 1$, normalisation is achieved by considering only monic polynomials. By the degree of a polynomial $A(X_1, \ldots, X_k)$ will be understood the ordered set $(m_1, \ldots, m_k)$, where m_i is the degree of $A(X_1, \ldots, X_k)$ in X_i $(i = 1, \ldots, k)$.

In [3], the author evaluated $N(m_1, \ldots, m_k)$, the total number of polynomials of degree $(m_1, \ldots, m_k)$ and, for $k \geqq 2$, obtained estimates for $\pi(m_1, \ldots, m_k)$ the number of irreducible (or prime) polynomials of the same degree. The value of $\pi(m_1, \ldots, m_k)$ when $k = 1$ is well-known. We proceed now to define functions $M, Q_r (r \geqq 2), D$ and Φ all of which have been evaluated by Carlitz [1], using a zeta-function method, when $k = 1$. Our aim is to estimate them for $k \geqq 2$. Let a typical, non-constant polynomial A in $GF[q, X_1, \ldots, X_t]$ have prime factorisation

$$A = P_1^{\alpha_1} \ldots P_t^{\alpha_t} \tag{1.1}$$

and define the functions $\mu(A)$ (" Möbius " function), $\mu_r(A) (r \geqq 2)$ and $d(A)$ on $GF[q, X_1, \ldots, X_k]$ as follows:

$$\mu(A) = \left\{ \begin{array}{l} 1, \text{ if } A = 1, \\ (-1)^t, \text{ if } \alpha_1 = \ldots = \alpha_t = 1, \\ 0, \quad \text{otherwise;} \end{array} \right\} \tag{1.2}$$

$$\mu_r(A) = \left\{ \begin{array}{l} 1, \text{ if } \alpha_i < r, i = 1, \ldots, t \text{ or if } A = 1, \\ 0, \quad \text{otherwise;} \end{array} \right\} \tag{1.3}$$

$$d(A) = \left\{ \begin{array}{l} 1, \text{ if } A = 1, \\ (\alpha_1 + 1) \ldots (\alpha_t + 1), \text{ otherwise.} \end{array} \right\} \tag{1.4}$$

In (1.2), (1.3) and (1.4), if $A \neq 1, A$ is assumed to have the form (1.1). Now put $M(m_1, \ldots, m_k) = \sum \mu(A), Q_r(m_1, \ldots, m_k) = \sum \mu_r(A)$ and $D(m_1, \ldots, m_k) = \sum d(A)$, where in each case the sum is over all polynomials of degree $(m_1, \ldots, m_k)$. Thus $Q_r(m_1, \ldots, m_k)$ is the number of " r-free " polynomials of degree $(m_1, \ldots, m_k)$ and, since $d(A)$ is just the number of divisors (including 1) of $A, D(m_1, \ldots, m_k)/N(m_1, \ldots, m_k)$ is the average number of divisors of polynomials of degree

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

$(m_1,\dots,m_k)$. Finally, let $\phi(A)$ ("Euler's" function) denote the number of polynomials relatively prime to and of the same degree as A and put $\Phi(m_1,\dots,m_k)=\sum\phi(A)$, where the sum is as before.

In our method, we employ formal power series in k indeterminates such as

$$Z(u_1,\dots,u_k)=\sum_{m_1=0}^{\infty}\dots\sum_{m_k=0}^{\infty}N(m_1,\dots,m_k)u_1^{m_1}\dots u_k^{m_k}. \tag{1.5}$$

Now for large values of $m_1,\dots,m_k$, $N(m_1,\dots,m_k)=O(q^{(m_1+1)\dots(m_k+1)})$. Hence if we regard (1.5) as a power series in k real variables $u_1,\dots,u_k$ and if $u_1\dots u_k\neq 0$, we see that $Z(u_1,\dots,u_k)$ is convergent only if $k=1$ and $|u_1|<q^{-1}$. Accordingly, we develop briefly a theory of purely formal power series. In [3] we proved the relation

$$m_1 N(m_1,\dots,m_k)=\sum_{s_1=0}^{m_1}\dots\sum_{s_k=0}^{m_k}s_1 L(s_1,\dots,s_k)N(m_1-s_1,\dots,m_k-s_k), \tag{1.6}$$

where, if $\pi(0,\dots,0)=0$,

$$L(m_1,\dots,m_k)=\sum_{j\mid(m_1,\dots,m_k)}j^{-1}\pi(m_1/j,\dots,m_k/j). \tag{1.7}$$

Relation (1.6) was first proved for $k=2$ by Carlitz [2]. In the paper cited, he also gives a proof of (1.6) for $k=2$ involving a formal use of the series (1.5). (In (1.7) and elsewhere the greatest common divisor $(m_1,\dots,m_k)$ of $m_1,\dots,m_k$, is to be distinguished from the degree $(m_1,\dots,m_k)$ by context.) Using our theory of power series, we derive various relations similar to (1.6), including one for each of the functions M, Q_r, D and Φ involving the function and N and one for each of M, Q_r and D involving the function and L (i.e., π). Using the relations involving N, and our knowledge of N, we obtain the required estimates.

In [3] we noted that, for $k=1$,

$$\pi(m)\sim m^{-1}N(m)\quad\text{as}\quad m\to\infty, \tag{1.8}$$

while, if $k\geqq 2$,

$$\pi(m_1,\dots,m_k)\sim(1-q^{1-n})N(m_1,\dots,m_k)\quad\text{as}\quad m_k\to\infty, \tag{1.9}$$

where n is defined for all $k\geqq 1$ by

$$n=(m_1+1)\dots(m_k+1)/(m_k+1). \tag{1.10}$$

Suppose that $k\geqq 2$ and that $m_{k-1}\to\infty$. Then $n\to\infty$ and so $q^{1-n}\to 0$. In view of this and (1.9), when $k\geqq 2$ we concentrate almost exclusively on the case when $m_1,\dots,m_{k-1}$ are considered fixed and $m_k\to\infty$. In spite of the dissimilarity of (1.8) and (1.9) we can state the results for Q_r, M and Φ simultaneously for all k. Thus we have, as $m_k\to\infty$

$$M(m_1,\dots,m_k)\sim-(1-q^{1-n})^2N(m_1,\dots,m_k),$$

$$Q_r(m_1,\dots,m_k)\sim(1-q^{1-rn})N(m_1,\dots,m_k),$$

$$\Phi(m_1,\dots,m_k)\sim(1-q^{1-2n})N^2(m_1,\dots,m_k).$$

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

On the other hand, it is inevitable from (1.8) and (1.9) that a separate statement is required for the two cases $k = 1$ and $k > 1$ in the estimate for $D(m_1, \ldots, m_k)$. We have, if $k = 1$, $D(m) = (m+1)N(m)$, while if $k \geqq 2$,

$$D(m_1, \ldots, m_k) \sim 2(1-q^{1-n})^{-1} N(m_1, \ldots, m_k) \quad \text{as} \quad m_k \to \infty.$$

For convenience, we shall subsequently abbreviate any function $U(m_1, \ldots, m_k)$ to $U(m_i)$ where possible. Similarly $\sum_{s_i=a_i}^{b_i}$ will mean $\sum_{s_1=a_1}^{b_1} \ldots \sum_{s_k=a_k}^{b_k}$, and the degree $(m_1, \ldots, m_k)$ of a polynomial will be written (m_i).

2. Formal power series. Let S_k be the set of all formal power series (f.p.s.) in k indeterminates, $u_1, \ldots, u_k$ of the form

$$F(u_1, \ldots, u_k) = \sum_{m_i=0}^{\infty} f(m_i) u_1^{m_1} \ldots u_k^{m_k}, \tag{2.1}$$

where $f(m_i)$ is a real valued function of the non-negative integer variables $m_1, \ldots, m_k$. From now on the f.p.s. (2.1) will be denoted by $F(u_i) = \sum f(m_i) u_i^{m_i}$. The f.p.s. with $f(0, \ldots, 0) = 1$ and $f(m_i) = 0$ otherwise will be denoted by I and the zero f.p.s. by 0. Let $G(u_i)$ be the f.p.s. $\sum g(m_i) u_i^{m_i}$ in S_k. We say $F = G$ if and only if $f(m_i) = g(m_i)$ for all integer sets $\{m_1, \ldots, m_k\}$, and $F+G$ is defined in the natural way. The product FG is defined to be the f.p.s. E, where

$$E(u_i) = F(u_i)G(u_i) = \sum e(m_i) u_i^{m_i}, \tag{2.2}$$

and $e(m_i)$ is the Cauchy product

$$e(m_i) = \sum_{s_i=0}^{m_i} f(s_i) g(m_i - s_i). \tag{2.3}$$

It is evident that, with the above operations, S_k is a commutative ring with identity I. Moreover, S_k is an integral domain and hence the cancellation law holds. To see this, suppose that F and G are non-zero f.p.s. in S_k. Then there exist sets $\{s_1, \ldots, s_k\}$ and $\{t_1, \ldots, t_k\}$ such that $f(s_i') = g(t_i') = 0$ if $\sum_{i=1}^{k} s_i' < \sum_{i=1}^{k} s_i$ and $\sum_{i=1}^{k} t_i' < \sum_{i=1}^{k} t_i$ but $f(s_i) \cdot g(t_i) \neq 0$. Let $m_i = s_i + t_i$, $i = 1, \ldots, k$. We have

$$e(m_i) = \sum_{r_i=0}^{m_i} f(r_i) g(m_i - r_i) = f(s_i) g(t_i) \neq 0. \tag{2.4}$$

It follows from (2.2), (2.3) and (2.4) that $FG \neq 0$.

Let F' denote the formal derivative of $F \in S_k$ with respect to u_1. Then trivially $(F+G)' = F' + G'$ and it is easy to verify by using (2.2) that $(FG)' = F'G + FG'$. This product rule extends in the usual way to the product of any number of f.p.s. In particular, if $r \geqq 1$, we have $(F^r)' = r(F^{r-1})F'$. Further it is obvious that if $r \geqq 1$ and $E(u_i) = F(u_i^r)$, then $E' = r u_1^{r-1} F'$.

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

For f.p.s. of a certain type we now extend the definition of product to that of an infinite number of f.p.s. Let χ be a real multiplicative function of $GF[q, X_1, \ldots, X_k]$, not identically zero. Thus $\chi(AB) = \chi(A)\chi(B)$ if $(A, B) = 1$ and $\chi(1) = 1$. For an irreducible P of degree (n_i) let $H_P(u_i)$ be the f.p.s.

$$H_P(u_i) = 1 + \chi(P)u_i^{n_i} + \chi(P^2)u_i^{2n_i} + \ldots = \sum_{\alpha=0}^{\infty} \chi(P^\alpha)(u_1^{n_1} \ldots u_k^{n_k})^\alpha \tag{2.5}$$

and define the product $H(u_i)$ of the $H_P(u_i)$ for all irreducible P to be

$$H(u_i) = \prod_P H_P(u_i) = \sum h(m_i)u_i^{m_i}, \tag{2.6}$$

where $h(m_i) = \sum \chi(A)$, the sum being over all polynomials of degree (m_i). Now suppose that χ_1 and χ_2 are non-zero multiplicative functions of $GF[q, X_1, \ldots, X_k]$ and that $J_P(u_i)$ and $K_P(u_i)$, respectively, are the corresponding f.p.s. of type (2.5). By (2.2), $J_P \times K_P = H_P$, where $H_P(u_i)$ has form (2.5) with $\chi(1) = 1$ and

$$\chi(P^\alpha) = \sum_{s=0}^{\alpha} \chi_1(P^s)\chi_2(P^{\alpha-s}) = \sum_{CD=P^\alpha} {}'\chi_1(C)\chi_2(D). \tag{2.7}$$

Extend χ to be a (non-zero) multiplicative function of $GF[q, X_1, \ldots, X_k]$. Thus $\prod_P (J_P \times K_P)$ has the form (2.6). It is of fundamental importance that we can write

$$(\prod_P J_P) \times (\prod_P K_P) = \prod_P (J_P \times K_P). \tag{2.8}$$

To prove (2.8), the coefficient of $u_i^{m_i}$ in the f.p.s. on the left side of (2.8) is, by (2.2) and (2.6),

$$\sum_{s_i=0}^{m_i} \left(\sum_{\deg C=(s_i)} \chi_1(C) \right) \left(\sum_{\deg D=(m_i-s_i)} \chi_2(D) \right) = \sum_{\deg A=(m_i)} \sum_{CD=A} \chi_1(C)\chi_2(D). \tag{2.9}$$

By (2.6) and (2.9) it is therefore sufficient to show that we can extend (2.7) to

$$\chi(A) = \sum_{CD=A} \chi_1(C)\chi_2(D). \tag{2.10}$$

The truth of (2.10) is established by using induction on the number t of distinct primes in A. The inductive step is, if A has form (1.1) with $t > 1$,

$$\chi(A) = \chi(AP_t^{-\alpha_t})\chi(P_t^{\alpha_t}) = \left(\sum_{C'D'=AP_t^{-\alpha_t}} \chi_1(C')\chi_2(D') \right) \left(\sum_{s=0}^{\alpha_t} \chi_1(P^s)\chi_2(P^\alpha t^{-s}) \right),$$

from which (2.10) follows. Thus (2.8) holds.

We remark finally that in what follows we shall use freely the properties of f.p.s. described in this section without specific mention.

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

3. Relations involving the functions. Let $Z_P(u_i)$ be the f.p.s. of type (2.5) with $\chi(A) = 1$ for all A. Accordingly, by (2.6) we have

$$Z(u_i) = \prod_P Z_P(u_i) = \sum N(m_i)u_i^{m_i}, \tag{3.1}$$

where, if $\deg P = (n_i)$,

$$Z_P(u_i) = 1 + u_i^{n_i} + u_i^{2n_i} + \dots. \tag{3.2}$$

Hence, by (3.1), if $\mathscr{L}(u_i)$ is the f.p.s. $u_1^{-1}\sum m_1 L(m_i)u_i^{m_i}$, where $L(m_i)$ is defined by (1.7), an expression equivalent to (1.6) is

$$Z'(u_i) = \mathscr{L}(u_i)Z(u_i). \tag{3.3}$$

We employ (3.3) in the sequel to derive relations involving L (i.e., π).

We now prove two relations involving $M(m_i)$.

THEOREM 1. *If $k \geqq 1$ and $m_1, \dots, m_k$ are non-negative integers not all zero, we have*

$$\sum_{s_i=0}^{m_i} M(s_i)N(m_i - s_i) = 0 \tag{3.4}$$

and

$$m_1 M(m_i) = -\sum_{s_i=0}^{m_i} s_1 L(s_i)M(m_i - s_i). \tag{3.5}$$

Proof. Let $\mathscr{M}_P(u_i)$ be the f.p.s. (2.5) with $\chi(A) = \mu(A)$. Thus, if $\deg P = (n_i)$, then $\mathscr{M}_P(u_i) = 1 - u_i^{n_i}$ and

$$\mathscr{M}(u_i) = \prod_P \mathscr{M}_P(u_i) = \sum M(m_i)u_i^{m_i}. \tag{3.6}$$

Now it follows from (3.2) and (2.2) that

$$\mathscr{M}_P(u_i)Z_P(u_i) = I.$$

Hence

$$\mathscr{M}(u_i)Z(u_i) = \prod_P (\mathscr{M}_P(u_i)Z_P(u_i)) = I. \tag{3.7}$$

Now differentiate (3.7) with respect to u_1. Clearly since $I' = 0$, we obtain, by (3.3),

$$\mathscr{M}'(u_i)Z(u_i) + \mathscr{M}(u_i)\mathscr{L}(u_i)Z(u_i) = 0,$$

i.e.,

$$\mathscr{M}'(u_i) = -\mathscr{L}(u_i)\mathscr{M}(u_i). \tag{3.8}$$

Statements (3.4) and (3.5) are now immediate from (3.7) and (3.8) by using (2.2). The proof is complete.

Statement (3.7) also leads to the following general inversion formula.

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

THEOREM 2. *Suppose that $f(m_i)$ and $g(m_i)$ are real functions of the non-negative integer variables $m_1, \ldots, m_k$ $(k \geqq 1)$ and that r is a positive integer. Then*

$$g(m_i) = \sum_{\substack{s_i=0 \\ r \mid (s_1, \ldots, s_k)}}^{m_i} N(s_i/r) f(m_i - s_i)$$

if and only if

$$f(m_i) = \sum_{\substack{s_i=0 \\ r \mid (s_1, \ldots, s_k)}}^{m_i} M(s_i/r) g(m_i - s_i).$$

Proof. Let $F(u_i)$ and $G(u_i)$ be the f.p.s. corresponding to $f(m_i)$ and $g(m_i)$ respectively. We then have

$$G(u_i) = Z(u_i^r)F(u_i) \Leftrightarrow G(u_i)\mathcal{M}(u_i^r) = \mathcal{M}(u_i^r)Z(u_i^r)F(u_i),$$

i.e.,

$$\Leftrightarrow F(u_i) = G(u_i)\mathcal{M}(u_i^r), \tag{3.9}$$

by (3.7). The result is immediate from (3.9). This completes the proof.

As an application of Theorem 2, we deduce from (1.6) an explicit formula for $\pi(m_i)$ in terms of $N(m_i)$ and $M(m_i)$. If $j \mid (m_1, \ldots, m_k)$, put $m_i = jn_i$, $i = 1, \ldots, k$. We then have

$$m_1 \pi(m_i) = \sum_{j \mid (m_1, \ldots, m_k)} \mu(j) \sum_{s_i=0}^{n_i} s_1 N(s_i) M(n_i - s_i), \tag{3.10}$$

where in (3.10), $\mu(j)$ is the ordinary Möbius function.

We consider now the function $Q_r(m_i)$.

THEOREM 3. *If $k \geqq 1$, $r \geqq 2$ and $m_1, \ldots, m_k$ are non-negative integers, we have*

$$N(m_i) = \sum_{\substack{s_i=0 \\ r \mid (s_1, \ldots, s_k)}}^{m_i} N(s_i/r) Q_r(m_i - s_i) \tag{3.11}$$

and

$$Q_r(m_i) = \sum_{\substack{s_i=0 \\ r \mid (s_1, \ldots, s_k)}}^{m_i} M(s_i/r) N(m_i - s_i). \tag{3.12}$$

Moreover, we have

$$m_1 Q_r(m_i) = \sum_{s_i=0}^{m_i} s_1 L(s_i) Q_r(m_i - s_i) - \sum_{\substack{s_i=0 \\ r \mid (s_1, \ldots, s_k)}}^{m_i} s_1 L(s_i/r) Q_r(m_i - s_i). \tag{3.13}$$

Proof. By Theorem 2, (3.12) follows from (3.11). To verify (3.11) and (3.13) let, for fixed $r \geqq 2$, $\mathcal{Q}_P(u_i)$ be the f.p.s. (2.5) with $\chi(A) = \mu_r(A)$. Hence $\mathcal{Q}_P(u_i) = 1 + u_i^{n_i} + \ldots + u_i^{(r-1)n_i}$ $(\deg P = (n_i))$ and

$$\mathcal{Q}_r(u_i) = \prod_P \mathcal{Q}_P(u_i) = \sum Q_r(m_i) u_i^{m_i}. \tag{3.14}$$

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

However,

$$\mathscr{Q}_P(u_i)Z_P(u_i^r) = (1+u_i^{n_i}+\ldots+u_i^{(r-1)n_i})(1+u_i^{rn_i}+u_i^{2rn_i}+\ldots) = Z_P(u_i). \tag{3.15}$$

It follows from (3.14) and (3.15) that

$$\mathscr{Q}_r(u_i)Z(u_i^r) = Z(u_i). \tag{3.16}$$

Differentiating (3.16) and using (3.3) and (3.16) yields

$$\mathscr{Q}_r'(u_i)Z(u_i^r)+ru_1^{r-1}\mathscr{Q}_r(u_i)\mathscr{L}(u_i^r)Z(u_i^r) = \mathscr{L}(u_i)Z(u_i) = \mathscr{L}(u_i)\mathscr{Q}_r(u_i)Z(u_i^r). \tag{3.17}$$

It follows from (3.17) that

$$\mathscr{Q}_r'(u_i) = \mathscr{L}(u_i)\mathscr{Q}_r(u_i)-ru_1^{r-1}\mathscr{L}(u_i^r)\mathscr{Q}_r(u_i). \tag{3.18}$$

(3.11) and (3.13) follow from (3.16) and (3.18) by equating coefficients of $u_i^{m_i}$. In particular, note that the coefficient of $u_1^{-1}u_i^{m_i}$ in $u_1^{r-1}\mathscr{L}(u_i^r)\mathscr{Q}_r(u_i)$ is

$$\sum_{\substack{s_i=0 \\ r\mid(s_1,\ldots,s_k)}}^{m_i} s_1/rL(s_i/r)Q_r(m_i-s_i).$$

The proof of the theorem is complete.

THEOREM 4. *If $k \geqq 1$ and $m_1,\ldots,m_k$ are non-negative integers, we have*

$$D(m_i) = \sum_{s_i=0}^{m_i} N(s_i)N(m_i-s_i) \tag{3.19}$$

and

$$m_1 D(m_i) = 2\sum_{s_i=0}^{m_i} s_1 L(s_i)D(m_i-s_i). \tag{3.20}$$

Proof. It is easy to prove (3.19) directly. Thus

$$D(m_i) = \sum_{\deg A=(m_i)}\sum_{CD=A} 1 = \sum_{s_i=0}^{m_i}\Big(\sum_{\deg C=(s_i)} 1\Big)\Big(\sum_{\deg D=(m_i-s_i)} 1\Big) \tag{3.21}$$

and (3.19) is immediate from (3.21). Now let $\mathscr{D}(u_i)$ be the f.p.s. $\sum D(m_i)u_i^{m_i}$. Then clearly (3.19) is equivalent to the expression

$$\mathscr{D}(u_i) = Z^2(u_i). \tag{3.22}$$

Differentiating (3.22) and using (3.3) leads to

$$\mathscr{D}'(u_i) = 2Z(u_i).Z(u_i)\mathscr{L}(u_i) = 2\mathscr{D}(u_i)\mathscr{L}(u_i), \tag{3.23}$$

by (3.22). From (3.23) we at once obtain (3.20). This proves the theorem.

Finally in this section we shall derive some relations involving N, Q_2, D and the function

$$W(m_i) = \sum_{\deg A=(m_i)} 2^{\omega(A)},$$

where $\omega(A)$ is the number of distinct prime divisors of A and $\omega(1) = 0$.

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

THEOREM 5. *If $k \geqq 1$ nd $m_1, \ldots, m_k$ are non-negative integers, we have*

$$W(m_i) = \sum_{s_i=0}^{m_i} N(s_i)Q_2(m_i - s_i) \tag{3.24}$$

and

$$D(m_i) = \sum_{\substack{s_i=0 \\ 2 \mid (s_1, \ldots, s_k)}}^{m_i} N(s_i/2)W(m_i - s_i). \tag{3.25}$$

Proof. This time choose $\chi(A) = 2^{\omega(A)}$ in (2.5) and let the corresponding f.p.s. be $\mathscr{W}_P(u_i)$. We have

$$\mathscr{W}(u_i) = \prod_P \mathscr{W}_P(u_i) = \sum W(m_i)u_i^{m_i},$$

where, if $\deg P = (n_i)$,

$$\mathscr{W}_P(u_i) = 1 + 2u_i^{n_i} + 2u_i^{2n_i} + \ldots.$$

On the other hand, if $r = 2$ in (3.14), we have

$$Z_P(u_i)\mathscr{Q}_P(u_i) = (1 + u_i^{n_i} + \ldots)(1 + u_i^{n_i}) = \mathscr{W}_P(u_i).$$

Hence

$$Z(u_i)\mathscr{Q}_2(u_i) = \mathscr{W}(u_i). \tag{3.26}$$

(3.24) follows from (3.26). Multiplying both sides of (3.26) by $Z(u_i^2)$ and using (3.16), we obtain

$$\mathscr{W}(u_i)Z(u_i^2) = Z^2(u_i) = \mathscr{D}(u_i) \tag{3.27}$$

and the assertion (3.25) follows from (3.27). The proof is complete.

We remark that further relations could be found from those of Theorem 5 by " inverting " and by using Theorem 2.

We note finally that it is possible to derive some of the results of this section directly using the technique of [3]. However, such proofs of (3.13) and (3.20), for example, are fairly lengthy.

4. Estimation of the functions. We turn now to the question of computing the functions we have defined.

For convenience, we shall often assume, without loss of generality, that if $k \geqq 2$ then $m_1, \ldots, m_{k-1}$ are non-negative integers satisfying

$$m_{k-1} = \max_{1 \leqq i \leqq k-1} m_i \geqq 1. \tag{4.1}$$

Hence if (4.1) holds and the integer R is defined by

$$R = \begin{cases} 0 & (k = 1), \\ nm_{k-1}(m_{k-1} + 1)^{-1} & (k \geqq 2), \end{cases} \tag{4.2}$$

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

where n is given by (1.10), then, if $k \geqq 2$,

$$R = \max_{1 \leqq i \leqq k-1} nm_i(m_i+1)^{-1}. \tag{4.3}$$

We state a lemma concerned with the value of $N(m_i)$. For proofs see [3].

LEMMA 1. *If $k \geqq 1$ and $m_1, \ldots, m_k$ are non-negative integers, we have*

$$(q-1)N(m_i) = \sum_{i=0}^{k} (-1)^i \sum^{(i)} q^{m_1 \ldots m_i(m_{i+1}+1)\ldots(m_k+1)}, \tag{4.4}$$

where $\sum^{(i)}$ denotes the sum over all different terms obtainable from the one shown by permutation of the m_j's. Moreover, if (4.1) *holds and R is given by* (4.2), *we have*

$$(q-1)N(m_i) = (q^n-1)q^{nm_k} + O(q^{Rm_k}), \tag{4.5}$$

where the implied constant is independent of m_k.

We shall use the following estimate of $N(s_i)N(m_i-s_i)$ several times. It is an immediate consequence of Lemmas 3 and 4 and statements (3.7) and (3.14) of [3].

LEMMA 2. *Suppose that $k \geqq 2$ and that $m_1, \ldots, m_k$ are non-negative integers such that* (4.1) *holds. If also $s_1, \ldots, s_k$ are integers satisfying*

$$0 \leqq s_i \leqq m_i \qquad (i = 1, \ldots, k)$$

for which $s_1, \ldots, s_{k-1}$ are not all zero and $s_i \neq m_i$ for all $i (i = 1, \ldots, k-1)$, then

$$N(s_i)N(m_i-s_i) = O(q^{Rm_k}), \tag{4.6}$$

where the implied constant is independent of m_k.

In fact, we could state a stronger result than that of Lemma 2, which informs us under what conditions we can replace $O(q^{Rm_k})$ in (4.6) by $O(q^{(R-1)m_k})$. In general this would lead to slight improvements in the error terms of results stated below. However, such improvements are gained only at the cost of fairly considerable detail and we merely state the improved result, where applicable. (Compare the proof of Theorem 2 in [3].)

We are now equipped to estimate the functions $M(m_i)$, $Q_r(m_i)$ and $D(m_i)$. We begin with $M(m_i)$. When $k = 1$, the result is in [1, §3].

THEOREM 6. *If $k \geqq 1$ and $m_1, \ldots, m_k$ are non-negative integers satisfying* (4.1) (*if $k \geqq 2$*), *then*

$$M(m_i) = -(1-q^{1-n})^2 N(m_i) + O(m_k q^{Rm_k}), \tag{4.7}$$

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

where the implied constant is independent of m_k. More precisely, if $k = 1$, we have

$$M(m) = \begin{cases} 1, & m = 0, \\ -q, & m = 1, \\ 0, & m \geqq 2. \end{cases} \tag{4.8}$$

Proof. We employ (3.4). First, suppose that $k = 1$. (4.8) is trivially true if $m = 0$ or 1. If $m \geqq 2$, we have, by (3.4),

$$0 = \sum_{s=0}^{m} M(s)q^{m-s} - q \sum_{s=0}^{m-1} M(s)q^{m-1-s} = M(m),$$

since $N(m) = q^m$. This proves (4.8) and hence (4.7) when $k = 1$.

Assume now $k \geqq 2$. By Lemma 2, we see that many of the terms in (3.4) are $O(q^{Rm_k})$ for large m_k, since it is obvious that $|M(m_i)| \leqq N(m_i)$. In fact, we have, if $m_k \geqq 1$,

$$\sum_{s=0}^{m_k} M(m_1, \ldots, m_{k-1}, s)N(0, \ldots, m_k - s) + \sum_{s=0}^{m_k} M(0, \ldots, 0, s)N(m_1, \ldots, m_k - s) = O(m_k q^{Rm_k}), \tag{4.9}$$

where the implied constant is independent of m_k. By (4.8), (4.9) becomes

$$\sum_{s=0}^{m_k} M(m_1, \ldots, m_{k-1}, s)q^{m_k - s} + N(m_1, \ldots, m_k) - qN(m_1, \ldots, m_{k-1}, m_k - 1) = O(m_k q^{Rm_k}). \tag{4.10}$$

Now if $m_k \geqq 2$ and we subtract from (4.10) the same expression with m_k replaced by $m_k - 1$ and with a factor q, we obtain

$$\begin{aligned} M(m_i) &= -N(m_1, \ldots, m_k) + 2qN(m_1, \ldots, m_{k-1}, m_k - 1) - q^2 N(m_1, \ldots, m_{k-1}, m_k - 2) \\ &\quad + O(m_k q^{Rm_k}) \\ &= -(1 - 2q^{1-n} + q^{2(1-n)})N(m_i) + O(m_k q^{Rm_k}), \end{aligned} \tag{4.11}$$

by (4.5). The result now follows from (4.11) and the proof is complete.

Using precise values of the N function given by (4.4) and (3.4), we can prove that, for large m,

$$M(2, m) = -(1 - q^{-2})^2 N(2, m) + (q - 1)(q^2 - 1)^2 m q^{2m-3} + O(q^{2m}). \tag{4.12}$$

Hence, by (4.12), (4.7) cannot, in general, be improved. However, apart from (4.12) and the corresponding expression for $M(1, 1, m)$, we can replace the error term in (4.7) by $O(q^{Rm_k})$.

We now estimate $Q_r(m_i)$. For $k = 1$ see also [1, §6].

THEOREM 7. *Let $r (\geqq 2)$ and $m_1, \ldots, m_k$ be non-negative integers such that* (4.1) *holds if $k \geqq 2$. Then*

$$Q_r(m_i) = (1 - q^{1-nr})N(m_i) + O(m_k q^{Rm_k}) \tag{4.13}$$

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

holds, where the implied constant is independent of m_k. *More precisely, if* $k = 1$, *the error term in* (4.13) *is* 0 *for* $m_k \geqq r$. *Otherwise.* $Q_r(m) = N(m)$.

Proof. This time we use (3.12). Suppose first that $k = 1$. Clearly we can also assume $m \geqq r$. By (3.12) and (4.8), we have

$$Q_r(m) = N(m) - qN(m-r)$$

and the theorem is proved for $k = 1$.

Assume now that $k \geqq 2$. Now clearly, if $r \mid (s_1, \ldots, s_k)$,

$$|M(s_i/r)| \leqq N(s_i/r) \leqq N(s_i).$$

Hence, by Lemma 2, if $s_1, \ldots, s_{k-1}$ are not all zero and $r \mid (s_1, \ldots, s_k)$,

$$M(s_i/r)N(m_i - s_i) = O(q^{Rm_k}) \tag{4.14}$$

for large m_k, except possibly if $s_i = m_i$, $i = 1, \ldots, k-1$ and $r \mid (m_1, \ldots, m_{k-1}, s_k)$. But in this latter case, by Lemma 1,

$$\begin{aligned} M(s_i/r)N(m_i - s_i) &\leqq N(s_i/r)q^{m_k - s_k} \\ &= O\{q^{((m_1/r)+1)\ldots((m_{k-1}/r)+1)(s_k/r)+m_k-s_k}\} \\ &= O(q^{(R/2)m_k + m_k}), \end{aligned} \tag{4.15}$$

since, by (4.1), $m_{k-1} \geqq r$ and $r \geqq 2$ and so $(m_{k-1}/r)+1 \leqq m_{k-1}$. Again using the fact that $m_{k-1} \geqq 2$ and hence $R \geqq 2$, we deduce from (4.15) that (4.14) is valid in this case also. It is now a consequence of (3.12) and (4.14) that, if $m_k \geqq r$,

$$\begin{aligned} Q_r(m_i) &= \sum_{\substack{s=0 \\ r \mid s}}^{m_k} M(0, \ldots, 0, s/r)N(m_1, \ldots, m_{k-1}, s) + O(m_k q^{Rm_k}) \\ &= N(m_1, \ldots, m_k) - qN(m_1, \ldots, m_{k-1}, m_k - r) + O(m_k q^{Rm_k}), \end{aligned} \tag{4.16}$$

by (4.8). The assertion (4.13) now follows from (4.16) by Lemma 1 and hence the theorem is proved.

We remark that in this instance the error term in (4.13) can be improved to $O(q^{Rm_k})$ in every case.

As indicated in §1, we require two statements concerning the value of $D(m_i)$ corresponding to the cases $k = 1$ and $k \geqq 2$. For another proof when $k = 1$, see [1, §4]. From the theorem, we have, as expected, $\lim_{m_{k-1} \to \infty} \lim_{m_k \to \infty} D(m_i) = 2$, when $k \geqq 2$.

THEOREM 8. *If* $k = 1$, *we have*

$$D(m) = (m+1)q^m. \tag{4.17}$$

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

If $k \geqq 2$ and $m_1, \ldots, m_k$ are non-negative integers such that (4.1) *holds, we have*

$$D(m_i) = 2(1-q^{1-n})^{-1}N(m_i)+O(m_k q^{Rm_k}), \tag{4.18}$$

where the implied constant is independent of m_k.

Proof. We employ (3.19). (4.17) is a trivial deduction from (3.19). Assume now that $k \geqq 2$. By (3.19) and Lemma 2, we have, for large m_k,

$$D(m_i) = 2\sum_{s=0}^{m_k} N(0,\ldots,0,m_k-s)N(m_1,\ldots,m_{k-1},s)+O(m_k q^{Rm_k})$$

$$= 2(q-1)^{-1}(q^n-1)q^{nm_k}\sum_{s=0}^{m_k} q^{(1-n)s}+O(m_k q^{Rm_k}),$$

by Lemma 1. Thus, since $n > 1$,

$$D(m_i) = 2(q-1)^{-1}(q^n-1)(1-q^{1-n})^{-1}(1-q^{(1-n)(m_k+1)})q^{nm_k}+O(m_k q^{Rm_k})$$
$$= 2(1-q^{1-n})^{-1}N(m_i)+O(m_k q^{Rm_k}),$$

by Lemma 1 again, which proves (4.17). This completes the proof.

Once again, we can improve the error term in (4.18) to $O(q^{Rm_k})$, except for $D(1, m)$, $D(2, m)$ and $D(1, 1, m)$. Thus we have, for example,

$$D(2,m) = 2(1-q^{-2})^{-1}N(2,m)+(q+1)^2 mq^{2m}+O(q^{2m}),$$

where the implied constant is independent of m.

We conclude this section with some remarks about Theorem 5. Suppose first that $k = 1$ and $m \geqq 2$. Then (3.24) and (4.8) yield

$$W(m) = \sum_{s=0}^{m-2}(1-q^{-1})q^s q^{m-s}+2q^m = [m(1-q^{-1})+(1+q^{-1})]N(m). \tag{4.19}$$

(4.19) implies that the average value of $2^{\omega(A)}$ for polynomials of degree $m(\geqq 2)$ is

$$m(1-q^{-1})+(1+q^{-1}) \sim m(1-q^{-1}) \quad \text{as} \quad m \to \infty.$$

Hence we would expect the average value of $\omega(A)$, (i.e., the average number of distinct prime divisors of A) to be $\sim c\log m (m \to \infty)$ for some constant c. In fact, $c = 1$ and the author intends including this result in a further paper. If now we assume that $k \geqq 2$, we can prove in a similar fashion to the proof of Theorem 8 that as $m_k \to \infty$

$$W(m_i) \sim \{2+2(1-q^{-n})(q^{n-1}-1)^{-1}\}N(m_i).$$

Thus the average value of $2^{\omega(A)}$ is $2+(1-q^{-n})(q^{n-1}-1)^{-1}$ and so the average value of $\omega(A)$ will be just greater than 1. A precise estimate will be given in the later paper.

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

5. The functions of Möbius and Euler. This section is mainly devoted to describing the properties of $\phi(A)$ defined in §1. We begin, however, with some remarks about the Möbius function $\mu(A)$. Exactly as in elementary number theory it can be shown that

$$\sum_{D \mid A} \mu(D) = \begin{cases} 1, & \text{if } A = 1, \\ 0, & \text{otherwise,} \end{cases}$$

holds and hence that, if $g(A)$ and $G(A)$ are real valued functions in $GF[q, X_1, \ldots, X_k]$, then

$$G(A) = \sum_{D \mid A} g(D) \Leftrightarrow g(A) = \sum_{CD = A} \mu(C) G(D) \tag{5.1}$$

is valid. This is the Möbius inversion formula.

It is natural to ask whether Euler's function $\phi(A)$ has analogous properties to the Euler's function of elementary number theory. When $k = 1$, the answer is yes, and the situation has been studied (see [1]). In this case it is easier to use an equivalent definition of $\phi(A)$ as being the number of polynomials (not necessarily monic or non-zero) whose degree is less than that of A, and which are prime to A. In other words $\phi(A)$ is the number of elements in a reduced system of residues (mod A). Thus, it is shown in [1] that $\phi(A)$ is multiplicative, i.e.,

$$\phi(AB) = \phi(A)\phi(B) \quad \text{when} \quad (A, B) = 1. \tag{5.2}$$

Moreover, if $\deg A = m$ and $|A| = q^m = N(m)$, $\phi(A)$ is given explicitly by

$$\phi(A) = |A| \prod_{P \mid A} (1 - |P|^{-1}), \tag{5.3}$$

where the product in (5.3) is over all prime divisors of A. Fundamental to the derivation of (5.3) is the fact that, when $k = 1$,

$$|AB| = |A||B|. \tag{5.4}$$

In the general case, when $k \geqq 1$, it is most natural to extend the definition of $|A|$ by putting $|A| = N(m_i)$, where $\deg A = (m_1, \ldots, m_k)$. If $k \geqq 2$, then by Lemma 1, (5.4) is certainly false with this definition of $|A|$. Hence (5.3) is also false, in general. For example, in place of (5.3), we can only say, if A has form (1.1), that

$$\phi(A) = \prod_{i=1}^{t} (|P^{\alpha_i}| - |P^{\alpha_i - 1}|). \tag{5.5}$$

To prove (5.5), note that ϕ is multiplicative since $(AB, C) = 1$ if and only if $(A, C) = 1$ and $(B, C) = 1$, and (5.2) follows if $(A, B) = 1$. It is also evident that $\phi(P^\alpha) = |P^\alpha| - |P^{\alpha-1}|$, where P is irreducible and $\alpha \geqq 1$. This proves (5.5). Another important relation, proved in a similar way to one proof of the corresponding result for positive integers is the following.

THEOREM 9. *We have*

$$\sum_{D \mid A} \phi(D) = |A|. \tag{5.6}$$

Moreover,

$$\phi(A) = \sum_{CD=A} \mu(C)\,|D|. \tag{5.7}$$

Proof. By (5.1), it is sufficient to prove (5.6). Let D be any divisor of A. Among the $|A|$ polynomials whose degree is that of A, consider those which are divisible by D. Let $A_1 D$ be any such polynomial. Then $A_1 D$ has highest common factor D with A if and only if $(A_1 D, A) = D$, i.e., if and only if $(A_1, A/D) = 1$. By the definition of ϕ, there are exactly $\phi(A/D)$ ways of choosing A_1, since $\deg A_1 = \deg(A/D)$. To summarise, we have shown that for any divisor D of A, there are exactly $\phi(A/D)$ polynomials whose degree is that of A and which have highest common factor D with A. Since each polynomial whose degree is $\deg A$ has a unique highest common factor with A, it follows that

$$\sum_{D \mid A} \phi(A/D) = |A|. \tag{5.8}$$

(5.6) follows at once from (5.8) and the theorem is proved.

We consider now the sum $\Phi(m_i)$ defined in §1.

THEOREM 10. *If $k \geqq 1$, we have, for non-negative integers $m_1, \ldots, m_k$,*

$$\Phi(m_i) = \sum_{s_i=0}^{m_i} M(s_i)\{N(m_i - s_i)\}^2.$$

Proof. We give a proof based on (5.7). We have

$$\Phi(m_i) = \sum_{\deg A=(m_i)} \sum_{CD=A} \mu(C)\,|D| = \sum_{s_i=0}^{m_i} \left\{ \sum_{\deg C=(s_i)} \mu(C) \right\} \left\{ \sum_{\deg D=(m_i-s_i)} |D| \right\}. \tag{5.9}$$

The assertion of the theorem follows from (5.9) by the definitions of $M(s_i)$ and $|D|$. The proof is complete.

Alternatively, we could prove Theorem 10 as follows without assuming the Möbius formula (5.1). We have, by (5.6),

$$\sum_{\deg A=(m_i)} \sum_{D \mid A} \phi(D) = \sum_{\deg A=(m_i)} |A| = N^2(m_i). \tag{5.10}$$

However,

$$\sum_{\deg A=(m_i)} \sum_{D \mid A} \phi(D) = \sum_{s_i=0}^{m_i} \left\{ \sum_{\deg C=(s_i)} 1 \right\} \left\{ \sum_{\deg D=(m_i-s_i)} \phi(D) \right\} = \sum_{s_i=0}^{m_i} N(s_i)\Phi(m_i - s_i). \tag{5.11}$$

Combining (5.10) and (5.11) leads to

$$N^2(m_i) = \sum_{s_i=D}^{m_i} N(s_i)\Phi(m_i - s_i) \tag{5.12}$$

and hence to Theorem 10 by Theorem 2. Conversely, we could deduce (5.12) from Theorem 10.

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

We require now a lemma which plays the same role as Lemma 2 in our previous investigations.

LEMMA 3. *Suppose that* $k \geqq 2$ *and that* $m_1, \ldots, m_k$ *are non-negative integers such that* (4.1) *holds. If, in addition,* $s_1, \ldots, s_k$ *are integers satisfying* $0 \leqq s_i \leqq m_i$ $(1 \leqq i \leqq k)$ *and* $s_1, \ldots, s_{k-1}$ *are not all zero, then*

$$N(s_i)\{N(m_i - s_i)\}^2 = O(q^{2Rm_k}),$$

where the implied constant is independent of m_k.

Proof. By Lemma 2, if $s_i \neq 0$ or m_i for all i $(i = 1, \ldots, k-1)$, then, for large m_k, we have

$$N(s_i)\{N(m_i - s_i)\}^2 = O(q^{Rm_k})N(m_i - s_i) = O(q^{2Rm_k}), \tag{5.13}$$

by Lemma 1, again using the fact that the s_i are not all zero $(i = 1, \ldots, k-1)$. It remains to establish (5.13) with $s_i = m_i$ $(1 \leqq i \leqq k-1)$. In this case we have, by Lemma 1,

$$\begin{aligned} N(s_i)\{N(m_i - s_i)\}^2 &= O(q^{n(s_k+1)+2(m_k-s_k)}) \\ &= O(q^{nm_k}) \\ &= O(q^{2Rm_k}) \end{aligned}$$

provided $2R \geqq n$, i.e., provided $m_{k-1} \geqq 1$, which we have assumed. Thus (5.13) holds and the lemma is proved.

We can now prove our estimate of $\Phi(m_i)$ valid for $k \geqq 1$. For another proof when $k = 1$, see [1, §5].

THEOREM 11. *If* $k \geqq 1$ *and* $m_1, \ldots, m_k$ *are non-negative integers satisfying* (4.1) (if $k \geqq 2$), *then*

$$\Phi(m_i) = (1 - q^{1-2n})N^2(m_i) + O(q^{(n+R)m_k}). \tag{5.14}$$

More precisely, when $k = 1$, *the error term in* (5.14) *is zero if* $m_k \geqq 1$.

Proof. When $k = 1$, substituting (4.8) in Theorem 10 yields, if $m \geqq 1$,

$$\Phi(m) = N^2(m) - qN^2(m-1) = (1 - q^{-1})q^{2m}.$$

This proves the theorem for $k = 1$. Assume now that $k \geqq 2$. Since, trivially, $|M(m_i)| \leqq N(m_i)$, we have, from Theorem 10 and Lemma 3,

$$\Phi(m_i) = \sum_{s=0}^{m_k} M(0, \ldots, 0, s)N^2(m_1, \ldots, m_{k-1}, m_k - s) + O(m_k q^{2Rm_k}), \tag{5.15}$$

where the implied constant is independent of m_k. Substituting (4.8) in (5.15) we obtain, if $m_k \geqq 1$,

$$\begin{aligned} \Phi(m_i) &= N^2(m_1, \ldots, m_k) - qN^2(m_1, \ldots, m_{k-1}, m_k - 1) + O(m_k q^{2Rm_k}) \\ &= (1 - q^{1-2n})N^2(m_1, \ldots, m_k) + O(q^{(n+R)m_k}), \end{aligned}$$

by Lemma 1. This completes the proof of the theorem.

https://doi.org/10.1017/S001708950000080X Published online by Cambridge University Press

In fact, it can be shown that, for large m,

$$\Phi(1, m) = (1-q^{-3})N^2(1, m)+2(q^2-1)q^{3m-3}+O(mq^{2m}),$$

so that, in general, (5.15) cannot be improved.

It is natural to define $p(m_i)$, the probability that two polynomials of degree $(m_1, \ldots, m_k)$ be relatively prime, as the ratio of relatively prime pairs to the number of all pairs of polynomials of degree $(m_1, \ldots, m_k)$. This leads to an alternative way of expressing the result of Theorem 11.

COROLLARY 12. *If $k \geqq 1$, we have*

$$\lim_{m_k \to \infty} p(m_i) = 1-q^{1-2n}.$$

Proof. If $m_k \geqq 1$, the total number of (distinct) pairs of polynomials of degree $(m_1, \ldots, m_k)$ is

$$\tfrac{1}{2}\{N^2(m_i)+N(m_i)\} \sim \tfrac{1}{2}N^2(m_i) \quad \text{as} \quad m_k \to \infty. \tag{5.16}$$

On the other hand the corresponding number of relatively prime pairs is

$$\tfrac{1}{2} \sum_{\substack{\deg M=(m_i) \\ (M, N)=1}} \sum_{\deg N=(m_i)} 1 = \tfrac{1}{2} \sum_{\deg M=(m_i)} \phi(M)$$

$$= \tfrac{1}{2}\Phi(m_i) \sim \tfrac{1}{2}(1-q^{1-2n})N^2(m_i) \tag{5.17}$$

as $m_k \to \infty$, by Theorem 11. The result follows from (5.10) and (5.17) and this completes the proof.

REFERENCES

1. L. Carlitz, The arithmetic of polynomials in a Galois field, *Amer. J. Math.* **54** (1932), 39–50.

2. L. Carlitz, The distribution of irreducible polynomials in several indeterminates II, *Canad. J. Math.* **17** (1965), 261–266.

3. S. D. Cohen, The distribution of irreducible polynomials in several indeterminates over a finite field, *Proc. Edinburgh Math. Soc.* **16** (1968), 1–17.

UNIVERSITY OF GLASGOW
GLASGOW, W.2.