Delta 3 (1972), 35-37.

PRODUCTS OF POLYNOMIALS OVER A FINITE FIELD

KENNETH S. WILLIAMS

(*Carleton University, Canada*)

The numbers 1, 2, ... , m include exactly $[m/p]$ multiples of the prime p, $[m/p^2]$ multiples of p^2, and so on. Hence we have the well-known result (see for example [2], page 342)

$$m\,! = \prod_{p} p^{\alpha(m,\,p)},$$

where

$$\alpha\,(m,\,p) = \sum_{s \geq 1} [m/p^s].$$

It is perhaps not so well-known that one can do a similar thing for polynomials over the finite field $GF(q)$. We consider $\prod_{\deg M = m} M$, where the product is over all monic polynomials M over $GF(q)$ of degree m. For any (monic) irreducible polynomial I over $GF(q)$, $\prod_{\deg M = m} M$ contains exactly $q^{m-\deg I}$ multiples of I, $q^{m-2\deg I}$ multiples of I^2, and so on. Hence we have

(1) $$\prod_{\deg M = m} M = \prod_{I} I^{\beta(m,\,I)},$$

where

$$\beta(m, I) = \sum_{s \geq 1} q^{m - s \deg I}. \tag{2}$$

Since $\beta(m, I)$ depends only on m and $\deg I$, writing

$$\gamma(m, i) = \sum_{s=1}^{[m/i]} q^{m-si} \quad (i = 1, 2, \ldots) \tag{3}$$

we can rewrite (1) as

$$\prod_{\deg M = m} M = \prod_{i=1}^{m} \left\{ \prod_{\deg I = i} I \right\}^{\gamma(m, i)} \tag{4}$$

This formula leads quickly to the well-known expression (see for example [1]) for the number $\pi_q(m)$ of monic irreducible polynomials of degree m over $GF(q)$. Equating degrees on both sides of (4) and using (3) we have

$$mq^m = \sum_{i=1}^{m} \sum_{s=1}^{[m/i]} q^{m-si}\, i\pi_q(i). \tag{5}$$

Collecting together the terms in (5) with the same value j for si we obtain

$$mq^m = \sum_{j=1}^{m} q^{m-j} \sum_{i/j} i\pi_q(i).$$

and so

$$q^m = mq^m - (m-1)q^m$$

$$= \sum_{j=1}^{m} q^{m-j} \sum_{i/j} i\pi_q(i) - q \sum_{j=1}^{m-1} q^{m-1-j} \sum_{i/j} i\pi_q(i),$$

that is

$$q^m = \sum_{i/m} i\pi_q(i). \tag{6}$$

Applying the Möbius inversion formula (see for example [2], page 236) to (6) we obtain

$$m\pi_q(m) = \sum_{i/m} \mu(m/i)q^i.$$

REFERENCES

1. **L. E. Dickson**, *Linear groups*, Dover, 1958, page 18.

2. **G.H. Hardy and E.M. Wright**, An Introduction to the Theory of Numbers, Oxford, 1962 edition.