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

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

It is perhaps not so well-known that one can do a similar thing for polynomials over the finite field GF(q). We consider $\prod_{\deg M} M$, where the product is over all monic polynomials M

over GF(q) of degree *m*. For any (monic) irreducible polynomial *I* over GF(q), $\prod_{\substack{\text{dog } M=m}} M$ contains exactly $q^{m-\deg I}$ multiples of *I*, *m-3* deg *I*

q multiples of I^2 , and so on. Hence we have

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

36

where

(2)
$$\beta(m, I) = \sum_{\sigma \ge 1} q^{m-\sigma \deg I}.$$

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

(3)
$$\gamma(m, i) = \sum_{m=1}^{[m/i]} q^{m-n} (i = 1, 2, ...)$$

we can rewrite (1) as

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

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

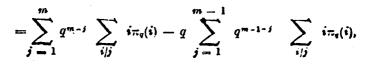
(5)
$$mq^{m} = \sum_{i=1}^{m} \sum_{q=1}^{[m/i]} q^{m-i} i \pi_{q}(i).$$

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

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



that is

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

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

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

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.