A POLYNOMIAL ANALOG OF THE GOLDBACH CONJECTURE[1]

BY DAVID HAYES

Communicated by G. B. Huff, September 28, 1962

We call a polynomial $c_0x^m+c_1x^{m-1}+\cdots+c_m$ in the ring $GF[q, x]$ *primary* if $c_0=1$. Suppose H is a polynomial in $GF[q, x]$ and let $h=\deg H$. Then the following theorem is easily established:

THEOREM 1. *If q is sufficiently large relative to h, then H is the sum of two irreducible polynomials, each of degree $h+1$.*

PROOF. The primary irreducibles of degree $h+1$ fall into $\phi(H)$ residue classes mod H. The number of such irreducibles is

$$\frac{q^{h+1}}{h+1}+O\left(\frac{q^{(h+1)/2}}{h+1}\right)$$

and the number of residue classes is $\phi(H)<q^h$. Therefore, if q is sufficiently large relative to h, some one residue class contains two irreducibles P and Q. For any such pair of irreducibles P and Q, there is an element α of $GF(q)$ so that $\alpha P+(-\alpha)Q=H$. This is the assertion of the theorem.

Our aim in this note is to sketch a proof of an asymptotic formula $(q\to\infty)$ for the number of representations of the polynomial H as a sum of two irreducibles, each of degree $h+1$. More specifically,

THEOREM 2. *Let $N(H)$ denote the number of pairs P, Q of primary irreducibles in $GF[q, x]$ such that*
(1) $\deg P=\deg Q=h+1$,
(2) $P\neq Q$,
(3) $P-Q\equiv 0 \pmod{H}$.
Then we have the asymptotic formula

$$N(H)=\frac{q^{2(h+1)}}{(h+1)^2\phi(H)}+O(q^{h+1}) \quad as \quad q\to\infty. \tag{1}$$

OUTLINE OF PROOF. Let $\pi(r; H, K)$ denote the number of primary irreducibles P of degree r such that $P\equiv K \pmod{H}$. Then we have

$$N(H)=\sum_K[\pi(h+1; H, K)]^2-\psi(h+1), \tag{2}$$

where K runs through a reduced residue system mod H, and $\psi(r)$ is

[1] Supported in part by NSF grant G-16485.