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

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

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.

the number of primary irreducibles in $GF[q, x]$ of degree r.

Let $\pi_K(r, d)$ denote the number of primary irreducibles P in $GF[q, x]$ such that

(1) $\deg P = r/d$,

(2) $P^d \equiv K \pmod{H}$

and let $D(r, K) = \sum_{d|r} (1/d)\pi_K(r, d)$. Note that $\pi_K(r, 1) = \pi(r; H, K)$. If $r < 2h$, we have $\pi_K(r, d) \leqq d$ for $d > 1$. Thus, we find that

$$D(r, K) - \pi(r; K, H) \leqq r, \tag{3}$$

for $r < 2h$.

According to a formula of Artin [1], we have

$$r\phi(H) D(r, K) = q^r - \sum_{\chi} \bar{\chi}(K) \sum_{i=1}^{m(\chi)} \beta_i^r(\chi) \tag{4}$$

where χ runs through all characters mod H and $m(\chi) \leqq h$. The numbers $\beta_i(\chi)$ for $1 \leqq i \leqq m(\chi)$ are closely associated with the zeroes of the L-function $L(s, \chi)$. The association is such that it follows from the Riemann hypothesis for algebraic function fields [2] that

$$|\beta_i(\chi)| \leqq hq^{1/2} \tag{5}$$

for all χ and $1 \leqq i \leqq m(\chi)$.

Using (3) and (4), we can show that

$$N(H) = \sum_K [D(h + 1, K)]^2 - \psi(h + 1) + O(q^{h+1}). \tag{6}$$

This last formula does not require (5). Also, after some manipulation, we derive from (4) and (5) the formula

$$\sum_K [D(h + 1, K)]^2 = \frac{q^{2(h+1)}}{(h + 1)^2\phi(H)} + O(q^{h+1}). \tag{7}$$

Combining (6) and (7) and making use of the trivial estimate $\psi(r) = O(q^r)$, we arrive at (1). This completes the proof.

REFERENCES

1. E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*. II, Math. Z. **19** (1924), 242–246.

2. A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind. No. 1041, Hermann, Paris, 1945, Deuxième Partie, §V.

DUKE UNIVERSITY