ARKIV FÖR MATEMATIK Band 3 nr 29

Communicated 25 January 1956 by T. NAGELL

Some theorems on polynomials

By L. CARLITZ

1. Let $F(x)=x^{2m}+a_1x^{2m-1}+\cdots+a_{2m}$ be a polynomial with rational coefficients. Let p be an odd prime that does not occur in the denominator of any a_r. Now assume that

$$F(x)\equiv G^2(x) \quad (\text{mod } p), \tag{1.1}$$

where $G(x)$ is a polynomial with integral coefficients (mod p). We may evidently suppose that

$$G(x)=x^m+b_1x^{m-1}+\cdots+b_m, \tag{1.2}$$

where the b_r are rational integers. Substituting from (1.2) in (1.1) we get a system of congruences

$$\begin{gathered} a_1\equiv 2b_1, \quad a_2\equiv b_1^2+2b_2, \quad a_3\equiv 2b_1b_2+2b_3, \\ a_4\equiv b_2^2+2b_1b_3+2b_4, \ \ldots \quad (\text{mod } p). \end{gathered} \tag{1.3}$$

There are of course $2m$ congruences in (1.3). Consider the first m of these. We may evidently choose rational numbers $b_1', \ldots, b_m'$ that are integral (mod p) and that satisfy the *equalities*

$$a_1=2b_1', \quad a_2=b_1'^2+2b_2', \ \cdots, \quad a_m=\cdots+2b_m'; \tag{1.4}$$

moreover $b_r'\equiv b_r$ (mod p) for $r=1, \ldots, m$. If we put

$$G'(x)=x^m+b_1'x^{m-1}+\cdots+b_m',$$

then $G'(x)\equiv G(x)$ (mod p) and (1.1) implies

$$F(x)=G'^2(x)+c_1x^{m-1}+c_2x^{m-2}+\cdots+c_m, \tag{1.5}$$

where the c_r are rational numbers that are integral (mod p); indeed

$$c_1\equiv c_2\equiv\cdots\equiv c_m\equiv 0 \ (\text{mod } p). \tag{1.6}$$

Comparing (1.5) with (1.4) it is clear that the c_r are completely determined by the a_r, that is by the polynomial $F(x)$ alone. Consequently if we assume that (1.1) holds for infinitely many primes p, it follows at once from (1.6) that all the c_r vanish. This proves the following result.[1]

Theorem 1. *Let the polynomial $F(x)$ with rational coefficients be congruent (mod p) to the square of a polynomial for infinitely many primes p. Then $F(x) = H^2(x)$, where $H(x)$ is a polynomial with rational coefficients.*

The proof of Theorem 1 evidently indicates that it suffices that (1.1) holds for a single sufficiently large p. More precisely we may state

Theorem 2. *Let the polynomial $F(x)$ be congruent (mod p) to the square of a polynomial, where $p > K_F$, a positive constant depending on $F(x)$. Then $F(x)$ is equal to the square of a polynomial $H(x)$ with rational coefficients.*

Indeed if the coefficients a_r of $F(x)$ satisfy

$$a_r = O(M^r) \qquad (r = 1, \ldots, 2m), \tag{1.7}$$

where the constant implied by O may depend on m and r, then it follows from (1.4) and (1.5) that

$$c_s = O(M^{m+r}) \qquad (s = 1, \ldots, m). \tag{1.8}$$

Thus we may take $K_F = kM^{m+1}$, where k depends only on m.

2. It is proved in [1] that if $F(x)$ is a polynomial (mod p) of degree m such that $F(a) \equiv b^2 \pmod{p}$ for all $a \pmod{p}$ and p exceeds a positive constant depending only on m, then $F(x) \equiv G^2(x) \pmod{p}$. Combining this result with Theorem 2 we get

Theorem 3. *Let the polynomial $F(x)$ satisfy*

$$F(a) \equiv b^2 \quad (\mathrm{mod}\ p), \tag{2.1}$$

for all a (mod p), where $b = b_a$ is an integer; also assume $p > K_F$, a positive constant depending on $F(x)$. Then $F(x)$ is equal to the square of a polynomial $H(x)$.

The remark following Theorem 2 applies here also.

It is clear that the above results may be generalized without difficulty to arbitrary powers.

3. In place of the rational field we may for example use an algebraic number field and of course replace the prime p by a prime ideal $\mathfrak{p}$; then the condition of Theorem 2 becomes $N\mathfrak{p} > K_F$. As for Theorem 3, we remark that the con-

[1] The writer has discussed this question with N. C. Ankeny.

dition $F(\alpha) \equiv \beta^2 \pmod{\mathfrak{p}}$ for all integral α again suffices for the application of [1, Theorem 1]. Hence Theorem 3 generalizes in the obvious way.

In the next place suppose that the coefficients a_r of $F(x)$ are in the field $GF(q, u)$, where u is an indeterminate. Now let $P(u)$ be an irreducible polynomial in $GF(q, u)$ that does not occur in the denominator of any a_r. Assume that

$$F(x) \equiv G^2(x) \qquad (\text{mod } P(u)), \tag{3.1}$$

where $G(x)$ is a polynomial in x with coefficients $\varepsilon\, GF(q, u)$. It is readily seen that the proof in § 1 carries over and we may accordingly state

Theorem 4. *Let* (3.1) *hold, where deg* $P(u) > K_F$, *a positive constant depending on* $F(x)$, *then* $F(x) = H^2(x)$, *where* $H(x)$ *is a polynomial with coefficients* $\varepsilon\, GF(q, u)$.

Corresponding to Theorem 3, the hypothesis (2.1) is now replaced by

$$F(f(u)) \equiv g^2(u) \qquad (\text{mod } P(u)), \tag{3.2}$$

where $f(u)$, $g(u)\,\varepsilon\, GF(q, u)$; indeed we assume that (3.2) holds for all $f(u)$, in other words for a complete residue system (mod $P(u)$). But since such a system constitutes the $GF(q^h)$, where $h = \deg P(u)$, it is clear that in this situation also, Theorem 1 of [1] applies. We have therefore

Theorem 5. *Let* (3.2) *hold for all* $f(u)\,\varepsilon\, GF[q, u]$ *of degree* $\leq h-1$, *where* $h = deg\ P(u) > k_F$, *a positive constant depending on* $F(x)$. *Then* $F(x)$ *is equal to the square of a polynomial with coefficients* $\varepsilon\, GF(q, u)$.

4. Returning to (1.1), if we modify this to read

$$F(x) \equiv G^2(x) H(x) \qquad (\text{mod } p) \qquad (\deg G(x) \geq 1), \tag{4.1}$$

then it follows at once that $p \mid d(F)$, the discriminant of $F(x)$. Hence if p is sufficiently large, $d(F) = 0$ and it follows that we have an equality

$$F(x) = G^2(x) H(x).$$

The same remark applies when (3.1) is modified in an analogous way.

Duke University.

REFERENCE

1. L. Carlitz, A problem of Dickson. Duke Mathematical Journal, vol. 19 (1952), pp. 471–474.

Tryckt den 5 september 1956

Uppsala 1956. Almqvist & Wiksells Boktryckeri AB