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

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

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

$$\begin{gathered} a_1\equiv 2b_1, \quad a_2\equiv b_1^2+2b_2, \quad a_3\equiv 2b_1b_2+2b_3, \\ a_4\equiv b_2^2+2b_1b_3+2b_4, \ \dots \pmod{p}. \end{gathered} \tag{1.3}$$

There are of course $2m$ congruences in (1.3). Consider the first m of these. We may evidently choose rational numbers $b_1', \dots, b_m'$ 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 $b_r'\equiv b_r \pmod{p}$ for $r=1, \dots, m$. If we put

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

then $G'(x)\equiv G(x) \pmod{p}$ 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

$$c_1\equiv c_2\equiv\cdots\equiv c_m\equiv 0 \pmod{p}. \tag{1.6}$$