ANNALS OF MATHEMATICS
Vol. 36, No. 4, October, 1935

ON THE FACTORIZATION OF POLYNOMIALS TO A PRIME MODULUS

BY MORGAN WARD

(Received December 4, 1934)

1. Let

$$A(x) = x^N - a_1x^{N-1} - a_2x^{N-2} - \cdots - a_N$$

be a polynomial in x with rational integral coefficients[1] and N distinct roots, $\alpha_1, \alpha_2, \cdots, \alpha_N$ and let p be a prime which does not divide its discriminant. Then we have a unique factorization modulo p:

$$A(x) \equiv A_1(x)A_2(x) \cdots A_r(x) \pmod p \tag{1.1}$$

where the polynomials $A_i(x)$ are all distinct, and all irreducible modulo p. I give here two formulas connecting the degrees of the polynomials $A_i(x)$ with the powers of p dividing certain of the numbers

$$\Delta_{(n)}(A) = \prod_{\nu=1}^{N} (\alpha_\nu^{p^n} - \alpha_\nu) = \text{Res}\,\{x^{p^n} - x, A(x)\}, n \text{ a positive integer.} \tag{1.2}$$

These numbers have been studied recently by D. H. Lehmer in another connection.[2]

2. Let $\mathfrak{A}$ denote the residue class of all polynomials of degree N which are congruent to $A(x)$ modulo p, and consider for each polynomial $A'(x)$ of $\mathfrak{A}$ the highest power of p which divides $\Delta_{(n)}(A') = \text{Res}\,\{x^{p^n} - x, A'(x)\}$. For a given value of n, this power is either zero for every such polynomial, or else a positive integer, which may be thought of as arbitrarily large if the resultant happens to vanish. If the power is not zero there clearly exist polynomials of $\mathfrak{A}$ for which it assumes a minimum value. We denote this minimum by p^{q_M}, so that we shall have for some polynomial $A'(x)$ of degree N,

$$\Delta_{(n)}(A') = p^{q_M} w, \qquad (p, w) = 1, \qquad A'(x) \equiv A(x) \pmod p,$$

while if $A''(x)$ is any other polynomial of degree N and congruent to $A(x)$ modulo p,

$$\Delta_{(n)}(A'') \equiv 0 \pmod{p^{q_M}}. \tag{2.1}$$

[1] This restriction will be understood in all that follows.

[2] These Annals, vol. 34, July 1933, pp. 461–479. The notation $\Delta_{(n)}(A)$ in place of the more natural $\Delta_{p^n}(A)$ is used for typographical reasons. With Lehmer's notation our $\Delta_{(n)}(A)$ would be written $(-1)^{N+1}a^N\Delta_{p^n-1}(A)$.

THEOREM 1. *The number T_M of irreducible factors $A_i(x)$ of $A(x)$ modulo p of degree M is given by the formula*

$$T_M = \frac{1}{M} \sum_{d|M} \mu(d) q_{M/d}. \tag{2.2}$$

THEOREM 2. *If p^{u_n} is the highest power of p dividing $\Delta_{(n)}(A)$, then $A(x)$ has an irreducible factor of degree M modulo p when and only when the integer*

$$s_M = \sum_{d|M} \mu(d) u_{M/d} \tag{2.3}$$

is positive.

In both theorems, $\mu(d)$ is Möbius' function, and the summation extends over all the divisors d of M.

3. As an illustration, consider the algebraically irreducible polynomial $A(x) = x^5 - 2x^3 + x^2 + 2x + 2$ for the case $p = 5$. We find by direct computation that the discriminant of $A(x)$ is congruent to 2 modulo 5, while $\Delta_{(1)}(A) \equiv 4$ modulo 5, $\Delta_{(2)}(A) \equiv 75$ modulo 125. Hence $r_1 = q_1 = 0$, $r_2 = q_2 = 2$, $T_1 = 0$, $T_2 = 1$, so that $A(x)$ has an irreducible quadratic factor (modulo 5), and no linear factors. Hence $A(x)$ must be the product of an irreducible cubic and an irreducible quadratic, (modulo 5). As a matter of fact

$$A(x) \equiv (x^2 + 2)(x^3 + x + 1) \pmod{5}.$$

4. In order to prove theorems 1 and 2, we need a chain of lemmas some of which are familiar (for example lemmas 4 and 5), while others contain results of a certain arithmetical interest in themselves. In any event, none of the proofs offer any difficulties, and they are accordingly omitted here.

Let $F(x)$ be any polynomial, and p any prime such that $F(x) \not\equiv 0 \pmod{p}$. Denote by τ, if it exists, the least positive value of n such that

$$x^{p^n} \equiv x \qquad (\text{modd } p, F(x)). \tag{4.1}$$

LEMMA 1. *$x^{p^n} \equiv x$ (modd p, $F(x)$) when and only when n is divisible by τ.*

LEMMA 2. If *$x^{p^\tau} \equiv x$ (modd p, $F(x)$) and $x^{p^\tau} - x$ is not exactly divisible by $F(x)$, so that there exists a positive integer s such that*

$$x^{p^\tau} \equiv x \quad (\text{modd } p^s, F(x)), \qquad x^{p^\tau} \not\equiv x \ (\text{modd } p^{s+1}, F(x)),$$

then if q is any positive integer,

$$x^{p^{q\tau}} \equiv x \quad (\text{modd } p^s, F(x)), \qquad x^{p^{q\tau}} \not\equiv x \ (\text{modd } p^{s+1}, F(x)).$$

LEMMA 3. *There exists no value of n for which*

$$x^{p^n} \equiv x \qquad (\text{modd } p, F^2(x)).$$

COROLLARY 3.1. *If the polynomial $F(x)$ has a squared factor, (4.1) is impossible for any positive n, and any prime p.*

COROLLARY 3.2. *If the prime p divides the discriminant of $F(x)$, (4.1) is impossible for any positive n.*

LEMMA 4. *If $F(x)$ is irreducible, modulo p, and if*

$$\Delta_{(n)} = \Delta_{(n)}(F) = \text{Res}\ \{x^{p^n} - x,\ F(x)\},$$

then $\Delta_{(n)} \equiv 0 \pmod p$ when and only when $x^{p^n} - x \equiv 0$ (modd p, $F(x)$).

LEMMA 5. *If $F(x)$ is an irreducible polynomial modulo p of degree M, then the least positive value of n for which (4.1) is satisfied is M.*

LEMMA 6. *If $F(x)$ is an irreducible polynomial modulo p of degree M, and if k is such that*

$$x^{p^k} \equiv x \qquad (\text{modd } p^2,\ F(x)),$$

then one can find an indefinite number of polynomials $F'(x)$ of degree M and congruent to $F(x)$ modulo p such that

$$x^{p^k} \equiv x \quad (\text{modd } p,\ F'(x)), \qquad x^{p^k} \not\equiv x \quad (\text{modd } p^2,\ F'(x)).$$

LEMMA 7. *If $F(x)$ is an irreducible polynomial modulo p of degree M, so that by lemma 5,*

$$x^{p^M} \equiv x \qquad (\text{modd } p,\ F(x)),$$

and if R is any assigned positive integer, it is possible to find a polynomial $F'(x)$ of degree M and congruent to $F(x)$ modulo p such that

$$x^{p^M} \equiv x \quad (\text{modd } p^R,\ F'(x)), \qquad x^{p^M} \not\equiv x \quad (\text{modd } p^{R+1},\ F'(x)).$$

LEMMA 8. *If $F(x)$ is an irreducible polynomial modulo p of degree M and if*

$$x^{p^k} \equiv x \quad (\text{modd } p^R,\ F(x)), \qquad x^{p^k} \not\equiv x \quad (\text{modd } p^{R+1},\ F(x)),$$

then

$$\Delta_{(k)}(F) \equiv 0 \pmod{p^{RM}}, \qquad \Delta_{(k)}(F) \not\equiv 0 \pmod{p^{RM+1}}.$$

LEMMA 9. *If $F(x)$ is a polynomial with no repeated roots, and if p is a prime which does not divide its discriminant, there exist positive values of n for which the congruence (4.1) holds.*

5. Let us return now to the congruence (1.1):

$$A(x) \equiv A_1(x)A_2(x) \cdots A_r(x) \pmod p.$$

By lemmas 6, 2 and 8, we can choose each $A_i(x)$ so that if $\Delta_{(M)}(A_i) =$ Res $\{x^{p^M} - x, A_i(x)\}$ is divisible by p, it is divisible by p^{d_i} and no higher power of p, where d_i is the degree of $A_i(x)$, and by lemmas 2, 5, and 8, $\Delta_{(M)}(A_i)$ is divisible by p when and only when d_i divides M. We may write therefore

$$\Delta_{(M)}(A_i) = p^{q_{M_i}} w_i, \qquad (p, w_i) = 1, \qquad (i = 1, 2, \cdots, r)$$

where

$$(5.1) \qquad q_{M_i} = d_i \quad \text{if } d_i \text{ divides } M; \qquad q_{M_i} = 0 \quad \text{otherwise.}$$

Let the $A_i(x)$ be chosen in this manner, and let

$$A_1(x)A_2(x) \cdots A_r(x) = \bar{A}(x).$$

Then $A(x) \equiv \bar{A}(x) \pmod{p}$, and the highest power of p dividing $\Delta_{(M)}(\bar{A})$ is

$$q_M = q_{M_1} + q_{M_2} + \cdots + q_{M_r}. \tag{5.2}$$

For

$$\Delta_{(M)}(\bar{A}) = \text{Res}\ \{x^{p^M} - x,\ \bar{A}(x)\} = \prod_{i=1}^{r} \text{Res}\ \{x^{p^M} - x,\ A_i(x)\} = \Delta_{(M)}(A_1) \cdots \Delta_{(M)}(A_r).$$

I say that p^{q_M} is the minimal power of p dividing $\Delta_{(M)}(A')$ for all polynomials $A'(x)$ of degree N which are congruent to $A(x)$ modulo p.

For given any such polynomial, and any positive integer L, by Schönemann's second theorem,[3] there exists a decomposition of $A'(x)$ modulo p^L of the form

$$A'(x) \equiv A'_1(x)A'_2(x) \cdots A'_r(x) \pmod{p^L}$$

where $A'_i(x)$ is congruent to $A_i(x)$ modulo p, and of the same degree in x. Therefore,

$$\Delta_{(M)}(A') \equiv \Delta_{(M)}(A'_1) \cdots \Delta_{(M)}(A'_r) \pmod{p^L}.$$

If u_{M_i} is the highest power of p dividing $\Delta_{(M)}(A'_i)$, we infer that the highest power of p dividing $\Delta_{(M)}(A')$ is

$$u_M = u_{M_1} + u_{M_2} + \cdots + u_{M_r},$$

for the integer L may be chosen arbitrarily large. Since $A'_i(x)$ is congruent to $A_i(x)$ and of the same degree, $u_{M_i} \geqq q_{M_i}$ so that $u_M \geqq q_M$.

Let T_d denote the total number of irreducible factors of $A(x)$ of degree d. Then by (5.1), (5.2) may be written

$$q_M = \sum_{d \mid M} dT_d. \tag{5.3}$$

Our first theorem now follows immediately by applying Dedekind's inversion formula to (5.3).[4]

6. To prove our second theorem, we construct a Schönemann decomposition of $A(x)$ itself modulo p^L similar to that of $A'(x)$ in section 5, obtaining successively

$$A(x) \equiv A''_1(x)A''_2(x) \cdots A''_r(x) \pmod{p^L},$$

$$\Delta_{(M)}(A) \equiv \Delta_M(A''_1)\Delta_M(A''_2) \cdots \Delta_M(A''_r) \pmod{p^L},$$

$$u_M = u_{M_1} + u_{M_2} + \cdots + u_{M_r}, \tag{6.1}$$

[3] Fricke, *Algebra*, vol. III, Braunschweig (1928), p. 67.

[4] Landau, *Vorlesungen über Zahlentheorie*, vol. I, Leipzig (1927), p. 22.

where $A_i''(x)$ is congruent to $A_i(x)$ modulo p, and of the same degree, and u_{M_i} is now the highest power of p dividing $\Delta_M(A_r'')$.

By lemma 2, u_{M_i} is zero unless the degree of $A_i''(x)$—that is, the degree of $A_i(x)$—divides M. We may write then

$$u_M = S_M + S_M'$$

where S_M is the contribution to the right side of (6.1) of all those irreducible factors $A_i''(x)$ of $A(x)$ modulo p^L of degree M, and S_M' the contribution of all the factors whose degrees are proper divisors of M. Thus S_M is different from zero when and only when $A(x)$ has at least one irreducible factor of degree M. From lemma 2, it is clear that

$$u_M = \sum_{d/M} s_d. \tag{6.2}$$

On applying Dedekind's inversion formula to (6.2), we obtain our second theorem.

7. If the factorization of $A(x)$ modulo p is known, q_M may be calculated by (5.3), and the minimal property of q_M gives us the congruence

$$\Delta_{(M)}(A) \equiv 0 \pmod{p^{q_M}}$$

In particular, if q_M is zero, $\Delta_{(M)}(A)$ is not divisible by p. We given in conclusion a formula for $\Delta_n(A) = \text{Res}\,\{x^n - x, A(x)\}$ which is useful in numerical applications; namely

$$\Delta_n(A) = \begin{vmatrix} W_n - W_0, & W_{n+1} - W_1, & \cdot & \cdot & W_{n+N-1} - W_{N-1}, \\ W_{n+1} - W_1, & W_{n+2} - W_2, & \cdot & \cdot & W_{n+N} - W_N, \\ \cdot \quad \cdot & \cdot \quad \cdot & \cdot & \cdot & \cdot \quad \cdot \\ \cdot \quad \cdot & \cdot \quad \cdot & \cdot & \cdot & \cdot \quad \cdot \\ W_{n+N-1} - W_{N-1}, & W_{n+N} - W_N, & \cdot & \cdot & W_{n+2N-2} - W_{2N-2}, \end{vmatrix}.$$

Here (W) is that solution of the difference equation

$$\Omega_{n+N} = a_1\Omega_{n+N-1} - a_2\Omega_{n+N-2} - \cdots - a_N\Omega_n$$

associated with the polynomial $A(x)$ with the initial values $W_0 = 0$,

$$W_1 = 0, \qquad W_2 = 0, \cdots, W_{N-2} = 0, \qquad W_{N-1} = 1.$$

The essential points in the proof of this formula will be found in a paper of mine in the Transactions of the American Mathematical Society.[5]

California Institute of Technology.

[5] Vol. 35, July (1933), page 608. The element in the lower right hand corner of the determinant $\Delta(U)$ given there should read u_{2k-2} instead of u_{2k-1}, and similarly for the determinant on page 604.