THE CANCELLATION LAW IN THE THEORY OF CONGRUENCES TO A DOUBLE MODULUS*

BY

MORGAN WARD

1. Let m be an integer greater than unity and $f(x)$ a fixed polynomial with integral coefficients.† If the leading coefficient of $f(x)$ is prime to m, then the quotient and remainder obtained on dividing any other polynomial by $f(x)$ have integral coefficients modulo m. Hence, as is well known, all polynomials may be separated into a finite number of residue classes $\mathfrak{A}, \mathfrak{B}, \cdots, \mathfrak{U}, \cdots$ which form a commutative ring‡ with respect to the operations of addition and multiplication (modulis $m, f(x)$). I propose here to determine what inferences can be drawn concerning the ring elements $\mathfrak{U}$ and $\mathfrak{V}$ from the ring equality $\mathfrak{A}\mathfrak{U}=\mathfrak{A}\mathfrak{V}$ when $\mathfrak{A}\neq 0$. Since $\mathfrak{A}\mathfrak{U}=\mathfrak{A}\mathfrak{V}$ is equivalent to $\mathfrak{A}(\mathfrak{U}-\mathfrak{V})=0$, we may assume that $\mathfrak{V}=0$. Stated in terms of congruences our problem is then equivalent to the following one:

Suppose that $f(x)=c_0x^k+c_1x^{k-1}+\cdots+c_k$ is a fixed polynomial with integral coefficients $c_0, \cdots, c_k$ and that m is an integer prime to c_0. Let $A(x)$ be a given polynomial such that

$$A(x) \not\equiv 0 \qquad (\text{modd } m, f(x)).$$

To determine all polynomials $U(x)$ such that

$$A(x)U(x) \equiv 0 \qquad (\text{modd } m, f(x)). \tag{1.1}$$

The problem is essentially a generalization of the problem of solving

$$au \equiv 0 \qquad (\text{mod } m)$$

for given integers a and m. Nevertheless it does not seem to have been considered heretofore save in very special cases.

I shall first of all show that it is sufficient to consider the case when m is a power of a prime p, say $m=p^N$, and when $f(x)$ is congruent modulo p to a power of an irreducible polynomial $\phi(x)$ (mod p);

$$f(x) = B(x) \equiv \{\phi(x)\}^\beta \qquad (\text{mod } p).$$

* Presented to the Society, August 31, 1932; received by the editors May 24, 1932.

† We shall restrict the term polynomial in what follows to mean a polynomial with integral coefficients.

‡ van der Waerden, *Moderne Algebra*, Berlin, 1930, vol. I, p. 37; Haupt, *Einführung in die Algebra*, Leipzig, 1929, vol. I, chapter V.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

This reduction corresponds to the fact that the ring associated with the moduli m and $f(x)$ is the direct sum of rings of the type associated with the moduli p^N and $B(x)$.

In this simpler case I shall show that there exists a positive integer λ and a set (S) of λ polynomials

$$A_0(x),\ A_1(x),\ \cdots,\ A_{\lambda-1}(x)$$

where λ and (S) depend only upon $A(x)$ and $B(x)$ and are independent of N, such that

$$A(x)U(x) \equiv 0 \qquad (\text{modd } p^N,\ B(x))$$

when and only when

$$U(x) \begin{array}{l} = p^{N-\lambda}(Q_0(x)A_0(x) + pQ_1(x)A_1(x) + \cdots + p^{\lambda-1}Q_{\lambda-1}(x)A_{\lambda-1}(x)) \text{ if } N = \lambda \\ = Q_{\lambda-N}(x)A_{\lambda-N}(x) + pQ_{\lambda-N+1}(x)A_{\lambda-N+1}(x) + \cdots + p^{N-1}Q_{\lambda-1}(x)A_{\lambda-1}(x) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } N \leqq \lambda, \end{array}$$

the polynomials $Q(x)$ being completely arbitrary, save for a restriction upon their degrees which we shall give later.

In the ring associated with the double modulus p^N, $B(x)$, our results are equivalent to the theorem that the ideal to which every element $\mathfrak{U}$ of the ring belongs which satisfies the relation

$$\mathfrak{A}\mathfrak{U} = 0$$

has a basis of the form

$$p^{N-\lambda}\mathfrak{A}_0,\ p^{N-\lambda+1}\mathfrak{A}_1,\ \cdots,\ p^{N-1}\mathfrak{A}_{\lambda-1} \quad \text{if} \quad N \geqq \lambda$$

or of the form

$$\mathfrak{A}_{\lambda-N},\ p\mathfrak{A}_{\lambda-N+1},\ \cdots,\ p^{N-1}\mathfrak{A}_{\lambda-1} \quad \text{if} \quad N \leqq \lambda,$$

where λ and $\mathfrak{A}_0, \cdots, \mathfrak{A}_{\lambda-1}$ depend only upon $\mathfrak{A}$, p and $B(x)$ and are independent of N.

2. Suppose that

$$m = p_1^{n_1} \cdots p_r^{n_r}$$

is the decomposition of m into its prime factors. Then it is readily seen that a necessary and sufficient condition that the congruence (1.1) hold is that the r congruences

$$A(x)U(x) \equiv 0 \qquad (\text{modd } p_i^{n_i}, f(x)),\ i = 1, \cdots, r, \tag{2.1}$$

hold. Furthermore, if we know the general solution $U^{(i)}(x)$ of each of the congruences (2.1), the general solution of the congruence (1.1) can be written

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

down immediately by means of the Chinese remainder theorem.* Hence it is sufficient to discuss the case when $m=p^N$, p a prime.

Let

$$f(x) \equiv c_0\{\phi_1(x)\}^{\beta_1} \cdots \{\phi_s(x)\}^{\beta_s} \pmod{p}, \quad (c_0, p) = 1,$$

be the decomposition of $f(x)$ into primary irreducible polynomials modulo p. Then by Schönemann's second theorem† there exists a decomposition of $f(x)$ modulo p^N of the type

$$f(x) \equiv c_0' B_1(x) \cdots B_s(x) \pmod{p^N}, (c_0', p) = 1,$$

where the polynomials $B_i(x)$ are primary, and

$$B_i(x) \equiv \{\phi_i(x)\}^{\beta_i} \pmod{p}, i = 1, \cdots, s. \tag{2.2}$$

Since $\operatorname{Res}\{B_i(x), B_j(x)\}$ is prime to p if $i \neq j$, it easily follows that (1.1) holds with $m=p^N$ when and only when the s congruences

$$A(x)U(x) \equiv 0 \quad (\text{modd } p^N, B_i(x)), i = 1, \cdots, s,$$

hold. If the solutions of these congruences are known, then the solution of the congruence (1.1) may be written down by the procedure of the Chinese remainder theorem.

It is sufficient then to study the congruence

$$A(x)U(x) \equiv 0 \quad (\text{modd } p^N, B(x)) \tag{2.3}$$

where

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \; B(x) = x^m + b_1x^{m-1} + \cdots + b_m$$

are given polynomials, p is a prime number, N a positive integer, and $U(x)$ is to be determined. Furthermore

$$B(x) \equiv \{\phi(x)\}^{\beta} \pmod{p} \tag{2.4}$$

where $\phi(x)$ is a primary irreducible polynomial modulo p and β a positive integer. We shall not need to use this last fact in what immediately follows. Finally, we lose no generality by requiring that $U(x)$ be of lesser degree than $B(x)$.

3. The first problem is to determine for a given N the highest power of p which divides every $U(x)$ satisfying (2.3). We shall show that there exists an integer λ depending only upon $A(x)$ and $B(x)$ such that if $N>\lambda$, every solution of (2.3) is divisible by $p^{N-\lambda}$, while if $N \leqq \lambda$, there exist solutions of

* Dickson, *Introduction to the Theory of Numbers*, Chicago, 1929, p. 10.

† For an account of Schönemann's theorems, see Fricke, *Algebra*, Braunschweig, 1928, vol. II, chapter 2.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

(2.3) which are not divisible by p. If $N>\lambda$, we may therefore write $U(x)=p^{N-\lambda}W(x)$ and thus reduce (2.3) to a congruence of the same form with $N=\lambda$. We shall see in the next section that the discussion of (2.3) when $N\leqq\lambda$ presents no difficulties whatsoever.

Let

$$E = E\begin{pmatrix} a_0, a_1, \cdots, a_n \\ 1, b_1, \cdots, b_m \end{pmatrix}$$

denote the $(m+n)$-rowed Sylvester eliminant of the polynomials $A(x)$ and $B(x)$, and let

$$\mathcal{E} = (e_{ij}) \qquad (i, j = 1, \cdots, m+n)$$

denote the transpose of the matrix of the determinant E.

Suppose that

$$E = p^L E' \quad \text{where} \quad L \geqq 0, \quad (p, E') = 1.$$

The congruence (2.3) is equivalent to an identity in x of the form

$$A(x)U(x) + B(x)V(x) = p^N W(x)$$

where the polynomial $V(x)$ is at most of degree $n-1$ and the polynomial $W(x)$ at most of degree $m+n-1$. If we denote the $m+n$ unknown coefficients of $U(x)$ and $V(x)$ in order by $z_1, z_2, \cdots, z_{m+n}$ and the coefficients of $W(x)$ by $w_1, w_2, \cdots, w_{m+n}$, then this identity is easily seen to be equivalent to the system of $m+n$ linear equations

$$\sum_{j=1}^{t} e_{ij}z_j = p^N w_i \qquad (i = 1, \cdots, t) \tag{3.1}$$

where for brevity we have written t for $m+n$. The determinant of this system is E; hence

$$Ez_j = p^N \sum_{i=1}^{t} \bar{e}_{ji}w_i \qquad (j = 1, \cdots, t),$$

$\bar{e}_{ji}$ denoting the co-factor of e_{ij} in E. Suppose that p^D is the highest power of p dividing all of the first minors $\pm\bar{e}_{ji}$ of E. Then on writing $p^L E'$ for E, we see that

$$E'z_j = p^{N+D-L} \sum_{i=1}^{t} e'_{ji}w_i \qquad (j = 1, \cdots, t)$$

where $p^D e'_{ji} = \bar{e}_{ji}$. At least one of the numbers e'_{ji} is not divisible by p; suppose that it is e'_{kl}. Then on taking w_l equal to 1 and the remaining w equal to 0,

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

we obtain a solution of (3.1) such that every z is divisible by p^{N+D-L} and at least one z, namely z_k, is not divisible by any higher power of p. It follows that the highest power of p dividing *all* solutions of (3.1) is p^{N+D-L}.

The integer p^{L-D} is simply the first elementary divisor of the matrix $\mathcal{E}$ corresponding to the prime factor p. Writing λ for $L-D$, we have the following result:

The least value of N such that every solution $U(x)$ of (2.3) of degree less than $B(x)$ should be divisible by p^T is $T+\lambda$, where p^λ is the first elementary divisor corresponding to the prime p of the matrix of the eliminant of $A(x)$ and $B(x)$.

Consequently, if $N \leqq \lambda$, there exist solutions of (2.3) which are not divisible by p, while if $N > \lambda$, every solution is divisible by $p^{N-\lambda}$. Since $\lambda = 0$ only when $L = D = 0$, we must have $U(x) \equiv 0 \pmod{p^N}$ if the resultant of $A(x)$ and $B(x)$ is prime to p. In the ring associated with p^N and $B(x)$, the corresponding case is when $\mathfrak{A}\mathfrak{U} = 0$ and $\mathfrak{A}$ is a unit of the ring.

4. We can now complete the discussion of the congruence (2.3). If $N > \lambda$, set $U(x) = p^{N-\lambda}W(x)$ thus obtaining the congruence for $W(x)$

$$A(x)W(x) \equiv 0 \qquad (\text{modd } p^\lambda, B(x)). \tag{4.1}$$

Among the polynomials $W(x)$ which satisfy (4.1) are some not divisible by p. Let $T(x)$ be such a one of lowest possible degree. Then the leading coefficient of $T(x)$ must be prime to p; for if not, by Schönemann's first theorem* there would exist a polynomial of the form $c+pQ(x)$ where c is prime to p such that $T(x)(c+pQ(x))$ would be congruent modulo p^λ to a polynomial $T'(x)$ of lower degree than $T(x)$. Then, since Res $\{c+pQ(x), B(x)\}$ is prime to p, we would have $A(x)T'(x) \equiv 0$ (modd p^λ, $B(x)$) contradicting our assumption about the degree of $T(x)$. On multiplying $T(x)$ by a constant prime to p, we obtain a polynomial $A_0(x)$ with leading coefficient unity and of minimal degree satisfying (4.1). *This polynomial is unique modulo p^λ*; for the difference of two such polynomials would be of lesser degree than either. Moreover if $W(x)$ is any solution of (4.1), the quotient and remainder obtained on dividing $W(x)$ by $A_0(x)$ have integral coefficients and the remainder being of lower degree than $A_0(x)$ must be divisible by p. Hence

$$W(x) = Q_0(x)A_0(x) + pW_1(x)$$

where $W_1(x)$ is of lesser degree than $A_0(x)$. On substituting this expression in (4.1), we obtain a congruence of the same form for $W_1(x)$:

$$A(x)W_1(x) \equiv 0 \qquad (\text{modd } p^{\lambda-1}, B(x)).$$

* Fricke, loc. cit., p. 59.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

We now repeat the previous argument. Every solution of this congruence must be of the form

$$W_1(x) = Q_1(x)A_1(x) + pW_2(x)$$

where $A_1(x)$ is a solution of minimal degree in x with leading coefficient unity uniquely determined modulo $p^{\lambda-1}$, while $W_2(x)$ is of lesser degree than $A_1(x)$.

We find on continuing in this manner that the general solution of (4.1) is of the form

$$W(x) = Q_0(x)A_0(x) + pQ_1(x)A_1(x) + \cdots + p^{\lambda-1}Q_{\lambda-1}(x)A_{\lambda-1}(x)$$

where the polynomial $A_i(x)$ is uniquely determined modulo $p^{\lambda-i}$.

We shall show in the next section that two consecutive polynomials $A_r(x)$ and $A_{r+1}(x)$ are equal only when all the polynomials $A_r(x)$, $A_{r+1}(x)$, $A_{r+2}(x), \cdots, A_{\lambda-1}(x)$ are equal, a circumstance which may occur for special choice of $A(x)$ and $B(x)$. If the degrees of $A_i(x)$ and $Q_i(x)$ are α_i and γ_i respectively, then it is clear that

$$\alpha_i - \alpha_{i+1} > \gamma_{i+1} \geqq 0 \qquad (i = 0, 1, \cdots, r-1).$$

The modification when the initial value of N is less than λ is obvious, and will be left to the reader. The results stated in the beginning of the paper are thus established.

5. We shall conclude by showing how the polynomials $A_{\lambda-1}(x)$, $A_{\lambda-2}(x)$, $\cdots, A_0(x)$ may be determined. We first observe that since

$$A(x)A_i(x) \equiv 0 \qquad (\text{modd } p^{\lambda-i}, B(x)) \tag{5.1}$$

we have $A(x)A_i(x) \equiv 0$ (modd $p^{\lambda-i-1}$, $B(x)$). Therefore by the fundamental property of $A_{i+1}(x)$,

$$A_i(x) \equiv 0 \qquad (\text{modd } p, A_{i+1}(x)) \qquad (i = 0, \cdots, \lambda-1). \tag{5.2}$$

We have seen in §2 that we may assume that $B(x)$ is of the form $\{\phi(x)\}^\beta + pV(x)$ where $\phi(x)$ is primary and irreducible modulo p. If we construct a Schönemann decomposition of $A(x)$ modulo p^N, it is easily seen that we may assume that $A(x)$ is of the same form; thus

$$B(x) = \{\phi(x)\}^\beta + pV(x), \quad A(x) = \{\phi(x)\}^\alpha + pR(x) \tag{5.3}$$

where $\alpha<\beta$, and the degrees of $V(x)$ and $R(x)$ are less than those of $B(x)$ and $A(x)$ respectively. Hence

$$A(x)\{\phi(x)\}^{\beta-\alpha} \equiv pR(x)\{\phi(x)\}^{\beta-\alpha} - pV(x) \qquad (\text{mod } B(x)).$$

If p^M is the highest power of p dividing the right side of this last congruence, we have

$$A(x)\{\phi(x)\}^{\beta-\alpha} \equiv 0 \qquad (\text{modd } p^M, B(x)), \not\equiv 0 \qquad (\text{modd } p^{M+1}, B(x))$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

and we may take

$$A_{\lambda-1}(x) = A_{\lambda-2}(x) = \cdots = A_{\lambda-M}(x),\ A_{\lambda-M}(x) \equiv \{\phi(x)\}^{\beta-\alpha} \pmod{p^M}.$$

Let i denote an integer $\leqq \lambda - M$. Then

$$A(x)A_i(x) \equiv p^{\lambda-i}S_i(x) \pmod{B(x)}, \tag{5.4}$$

where $S_i(x)$ is of lesser degree than $B(x)$.

We may assume that $S_i(x)$ *is not divisible by* p *and is of lesser degree than* $A(x)$. For since $A_i(x)$ is determined only modulo $p^{\lambda-i}$, if $S_i(x) = pS_i'(x)$ we have

$$A(x)(A_i(x) + p^{\lambda-i}) \equiv p^{\lambda-i}(A(x) + pS_i'(x)) \pmod{B(x)}$$

and by (5.3), the polynomial multiplying $p^{\lambda-i}$ on the right is not divisible by p. In the same way, if $S_i(x) = Q(x)A(x) + S_i''(x)$ where $S_i''(x)$ is of lesser degree than $A(x)$, then $Q(x)$ is necessarily of lesser degree than $A_i(x)$ so that $A_i(x) + p^{\lambda-i}Q(x)$ is a primary polynomial such that

$$A(x)(A_i(x) + p^{\lambda-i}Q(x)) \equiv p^{\lambda-i}S_i''(x) \pmod{B(x)}.$$

If $A_i(x)$ *is known, we can determine* $A_{i-1}(x)$. For, by (5.2),

$$A_{i-1}(x) = Q(x)A_i(x) + pR(x)$$

where $Q(x)$ must be primary, and $R(x)$ of lesser degree than $A_i(x)$. By (5.4),

$$A(x)A_{i-1}(x) \equiv p^{\lambda-i}Q(x)S_i(x) + pR(x)A(x) \pmod{B(x)}.$$

Take $R(x) = p^{\lambda-i-1}$. Then

$$A(x)A_{i-1}(x) \equiv 0 \quad (\text{modd } p^{\lambda-i+1}, B(x))$$

when and only when

$$Q(x)S_i(x) + A(x) \equiv 0 \quad (\text{modd } p, B(x)),$$

that is, when and only when

$$Q(x)S_i(x) + \{\phi(x)\}^{\alpha} \equiv 0 \quad (\text{modd } p, \{\phi(x)\}^{\beta}).$$

Since $S_i(x)$ is known and is of lesser degree than $\{\phi(x)\}^{\alpha}$ and not divisible by p, there exists a primary polynomial $Q(x)$ uniquely determined modulo p which satisfies this congruence. $A_{i-1}(x)$ is now uniquely determined modulo $p^{\lambda-i+1}$ and may be modified so as to satisfy the conditions corresponding to those imposed upon $A_i(x)$ in (5.4).

The remaining polynomials $A_{\lambda-M-1}(x), \cdots, A_1(x), A_0(x)$ can therefore be calculated step by step, and our solution is completed.

California Institute of Technology,
Pasadena, Calif.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use