ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 5, Number 2, Spring 1975

SOME ELEMENTARY NUMBER THEORETIC IMPLICATIONS OF THE SYMMETRIC FUNCTIONS THEOREM

C. H. KIMBERLING

1. **Introduction.** Our purpose in this paper is to present some elementary applications of the symmetric functions theorem which are difficult or impossible to find in the literature. Perhaps the closest reference is the recent expository paper of Gerst and Brillhart [3], which the interested reader will certainly want to consult.

The present paper consists of Theorem 1 below and some implications of that theorem: (1) if ζ is an integer in the cyclotomic field $Q(\xi)$, where ξ is a primitive nth root of unity, then the norm of ζ in $Q(\xi)$ is congruent to 0 or 1 modulo each prime divisor of n; (2) a similar result holds for determinants of circulants; (3) under cyclic permutations of coefficients within their factors, certain products remain congruent mod k; (4) if α and β are in a certain class of algebraic integers, a condition is found under which a prime p divides the discriminants of $\alpha + \beta$ and $\alpha\beta$.

Another implication of Theorem 1 is an extension of ordinary congruence mod q for rational integers to a larger class of algebraic integers. The main idea is suggested by defining $i \equiv 1 \bmod 2$, since $x^2 + 1 \equiv (x - 1)^2 \bmod 2$. Theorem 1 leads to conditions under which $\beta \equiv \alpha \bmod p$ and $\delta \equiv \gamma \bmod p$ imply $\beta + \delta \equiv \alpha + \gamma \bmod p$ and $\beta\delta \equiv \alpha\gamma \bmod p$, etc. A generalization of Fermat's theorem is obtained.

Throughout, let I = rational integers, I^+ = positive rational integers, and $p = a$ prime in I^+. Let $\alpha, \beta, \gamma, \delta$ denote algebraic integers and let polynomials in $I[x]$, always assumed monic, be written as follows:

$$a(x) = \prod_{i=1}^{m} (x - \alpha_i), \quad b(x) = \prod_{i=1}^{m} (x - \beta_i),$$

$$c(x) = \prod_{i=1}^{n} (x - \gamma_i), \quad d(x) = \prod_{i=1}^{n} (x - \delta_i).$$

Only when explicitly stated shall we assume that $a(x)$, $b(x)$, $c(x)$, $d(x)$ are the *minimal* polynomials of the roots α, β, γ, δ, where $\alpha_1 = \alpha$, $\beta_1 = \beta$, etc. The notation $b(x) \equiv a(x) \bmod q$ means that, when $b(x)$

Received by the editors April 10, 1973 and in revised form September 4, 1973.
This research was supported by University of Evansville Alumni Research Grant B6D-0240.

and $a(x)$ are written out as $b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + x^n$ and $a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + x^m$, we have $n = m$ and $b_i \equiv a_i \bmod q$ for $i = 0, 1, \cdots, m - 1$.

2. **Main theorem.** First we shall state without proof an easy consequence of the symmetric functions theorem:

LEMMA 1a. *Suppose* $q \in I^+$ *and* $b(x) \equiv a(x) \bmod q$. *Suppose* $\tau(x_1, \cdots, x_m)$ *and* $\sigma(x_1, \cdots, x_m)$ *are symmetric polynomials in* $I[x_1, \cdots, x_m]$ *having the same form, such that each coefficient in* $\tau(x_1, \cdots, x_m)$ *is congruent* $\bmod q$ *to the corresponding coefficient in* $\sigma(x_1, \cdots, x_m)$. *Then*

$$\tau(\beta_1, \cdots, \beta_m) \equiv \sigma(\alpha_1, \cdots, \alpha_m) \bmod q.$$

THEOREM 1. *Suppose* $q \in I^+$ *and* $b(x) \equiv a(x) \bmod q$ *and* $d(x) \equiv c(x) \bmod q$. *Then*

$$(1) \qquad \prod_{j=1}^{n} \prod_{i=1}^{m} [x - f(\beta_i, \delta_j)] \equiv \prod_{j=1}^{n} \prod_{i=1}^{m} [x - f(\alpha_i, \gamma_j)] \bmod q$$

for every polynomial $f(x, y)$ *in* $I[x, y]$.

PROOF. Rewrite (1) as

$$t_0 + t_1x + \cdots + x^{mn} \equiv s_0 + s_1x + \cdots + x^{mn} \bmod q.$$

Each t_k is symmetric in the β_i's and in the δ_j's. Thus, regarding the δ_j's as indeterminants, we have t_k expressible as a polynomial in $\delta_1, \cdots, \delta_n$ in which each coefficient, as a symmetric polynomial of the β_i's, is an integer. By Lemma 1a, this integer is congruent $\bmod q$ to the corresponding coefficient in s_k expressed as a polynomial in $\gamma_1, \cdots, \gamma_n$. Thus each t_k is a symmetric polynomial of $\delta_1, \cdots, \delta_n$ and within congruence $\bmod q$, s_k is the same polynomial of $\gamma_1, \cdots, \gamma_n$. Lemma 1a applies again and we conclude that $t_k \equiv s_k \bmod q$ for $k = 0, 1, \cdots, mn - 1$.

Theorem 1 and its implications which follow have generalizations to more than two pairs of numbers α, β and γ, δ at a time and also to congruences modulo prime ideals in coefficient rings.

THEOREM 2. *Suppose* $q \in I^+$ *and* $b(x) \equiv a(x) \bmod q$. *Then*

$$\prod_{i=1}^{m} [x - f(\beta_i)] \equiv \prod_{i=1}^{m} [x - f(\alpha_i) \bmod q$$

for every $f(x)$ *in* $I[x]$.

PROOF. Put $d(x) = c(x) = x$ in Theorem 1.

COROLLARY 2a. *Suppose* $n \geqq 2$ *and* ξ *is a primitive* nth *root of unity. Suppose* p *is a prime which divides* n *and* ζ *is an integer in the cyclotomic field* $Q(\xi)$. *Let* $N(\zeta)$ *denote the norm of* ζ *in* $Q(\xi)$. *Then* $N(\zeta) \equiv 0 \bmod p$ *or* $N(\zeta) \equiv 1 \bmod p$.

PROOF. Write $n = p^r k$ where $p \nmid k$. Let $F_n(x)$ denote the nth cyclotomic polynomial. Then

$$F_n(x) \equiv [F_k(x)]^{\phi(p^r)} \bmod p, \tag{2}$$

as proved in [4]. In terms of the conjugates $\xi = \xi_1, \xi_2, \cdots, \xi_{\phi(n)}$ of ξ and the conjugates $\eta_1, \eta_2, \cdots, \eta_{\phi(k)}$ of a primitive kth root η_1 of unity, (2) becomes

$$\prod_{i=1}^{\phi(n)} (x - \xi_i) \equiv \left[\prod_{i=1}^{\phi(k)} (x - \eta_i) \right]^{\phi(p^r)} \bmod p.$$

Now the conjugates of ζ in $Q(\xi)$ are given by $\zeta_i = f(\xi_i)$ for some $f(x)$ in $I[x]$, since ξ and its powers form an integral basis for $Q(\xi)$. See, for example, Pollard [6], pp. 67–70. By Theorem 2,

$$\prod_{i=1}^{\phi(n)} (x - \zeta_i) \equiv \prod_{i=1}^{\phi(k)} [x - f(\eta_i)]^{\phi(p^r)} \bmod p.$$

For $x = 0$, we have $N(\zeta)$ on the left and K^{p-1} on the right, where K is a rational integer. By Fermat's theorem, K^{p-1} reduces mod p to 0 or 1.

In passing, let us note a similar result which follows immediately from (2) and Fermat's theorem: For every integer k, we have $F_n(k) \equiv 0 \bmod p$ or $F_n(k) \equiv 1 \bmod p$.

We illustrate Corollary 2a with an example. For ξ a primitive fifth root of unity and $\zeta = a + b\xi + c\xi^2 + d\xi^3$, the norm of ζ is the determinant

$$\begin{vmatrix} a & b & c & d \\ -d & a-d & b-d & c-d \\ d-c & -c & a-c & b-c \\ c-b & d-b & -b & a-b \end{vmatrix},$$

which (along with being positive except in one case) is $\equiv (a + b + c + d)^4 \bmod 5$. (For the definition of norm as a determinant, see [7], p. 130.)

COROLLARY 2b. *Let* $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in I[x]$ *where* $n = \phi(k)$ *and* k *is* 2 *or an odd prime or twice a Fermat prime* $2^{2^t} + 1$. *Let* $r_1, \cdots, r_n$ *be the positive integers less than and relatively prime to* k. *Then the determinant of the circulant*

$$C = \begin{pmatrix} c_0 & c_1 & & c_{n-1} \\ c_{n-1} & c_0 & & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 \cdots & c_{n-3} \\ \vdots & & & \vdots \\ c_1 & c_2 & & c_0 \end{pmatrix}$$

satisfies $|C| \equiv \prod_{i=1}^{n} c(r_i) \bmod k$.

PROOF. The characteristic roots of C are $c(\xi_i)$, $i = 1, \cdots, n$, where the ξ_i's are the roots of $x^n = 1$ (e.g., [1], p. 242). Applying Theorem 2 to

$$x^n - 1 \equiv \prod_{i=1}^{n} (x - r_i) \bmod k$$

gives

$$\prod_{i=1}^{n} [x - c(\xi_i)] \equiv \prod_{i=1}^{n} [x - c(r_i)] \bmod k.$$

(A reference for the case of composite k is [2], p. 87, bottom, where it is to be noted that primes of the form $2^i + 1$ for $i = 0, 1, \cdots$, are 2 and the Fermat primes $2^{2^t} + 1$.) The required result follows for $x = 0$.

COROLLARY 2c. *Given the notation of Corollary* 2b, *let*

$$\hat{c}(x) = c_0 + c_{n-1}x + c_{n-2}x^2 + \cdots + c_2x^{n-2} + c_1x^{n-1}$$

and let

$$c^{(m)}(x) = c_{n-m} + c_{n-m+1}x + \cdots + c_{n-m-1}x^{n-1}$$

for $m = 1, 2, \cdots, n - 1$, *where* $c_n = c_0$, $c_{n+1} = c_1, \cdots, c_{2n-1} = c_{n-1}$. *Then*

$$(-1)^m \prod_{i=1}^{n} c^{(m)}(r_i) \equiv \prod_{i=1}^{n} c(r_i) \equiv (-1)^m \prod_{i=1}^{n} \hat{c}^{(m)}(r_i) \bmod k$$

for all $c(x)$ *of degree* $\leqq n - 1$ *in* $I[x]$ *and* $m = 1, 2, \cdots, n - 1$.

PROOF. We have $\prod_{i=1}^{n} c(r_i) \equiv |C| \bmod k$. An odd number of row transpositions converts C into the circulant $C^{(1)}$ with top row $(c_{n-1}, c_0, c_1, \cdots, c_{n-2})$. Thus $(-1)|C^{(1)}| = |C|$. By Corollary 2b,

$$|C^{(1)}| \equiv \prod_{i=1}^{n} c^{(1)}(r_i) \bmod k.$$

The rest of the proof for $c^{(m)}$ follows by induction, since $C^{(m+1)}$ comes from $C^{(m)}$ for $m = 1, 2, \cdots, n-1$ as does $C^{(1)}$ from C. For $\hat{c}^{(m)}$, note that the transpose of C is the circulant whose top row consists of the coefficients of $\hat{c}(x)$ in order. Thus the argument above applies to $\hat{c}^{(m)}$.

3. **A Congruence Relation for Algebraic Integers.**

DEFINITIONS. 1. For $r \in I^+$, let I_r be the set of algebraic integers whose degree divides r. If α in I_r has minimal polynomial $a(x)$ of degree m, then the *r-polynomial for* α is $[a(x)]^{r/m}$, henceforth written $a^r(x)$.

2. For r and q in I^+, define $\overset{r}{\equiv} \bmod q$ in I_r as follows:

$$\beta \overset{r}{\equiv} \alpha \bmod q \text{ if } b^{(r)}(x) \equiv a^{(r)}(x) \bmod q,$$

where $b(x)$ and $a(x)$ are the minimal polynomials of β and α, respectively. Whenever $\beta \overset{r}{\equiv} \alpha \bmod q$ for $r = \max(\deg \beta, \deg \alpha)$, we shall write merely $\beta \equiv \alpha \bmod q$. For example, primitive pth roots of unity satisfy $\xi \equiv 1 \bmod p$, primitive $2p$th roots of unity satisfy $\xi \equiv -1 \bmod p$, and primitive 12th roots of unity satisfy $\xi \equiv i \bmod 3$.

Clearly $\overset{r}{\equiv} \bmod q$ is an equivalence relation in I_r and generalizes the congruence relation $\equiv \bmod q$ in I.

LEMMA 3a. *Suppose $b(x)$ and $c(x)$ are monic polynomials in $I[x]$ and $a_1(x), \cdots, a_j(x)$, also monic in $I[x]$, are irreducible* mod p. *If*

$$b(x)c(x) \equiv \prod_{i=1}^{j} a_i(x) \bmod p, \text{ then } b(x) \equiv \prod_{\ell=1}^{k} a_{i_\ell}(x) \bmod p$$

for some subset $\{i_1, \cdots, i_k\}$ of $\{1, \cdots, j\}$.

For a proof, see [5], p. 96.

THEOREM 3. *Suppose $\beta \overset{r}{\equiv} \alpha \bmod p$ and $\delta \overset{s}{\equiv} \gamma \bmod p$. Suppose $f(x, y) \in I[x, y]$ and that the minimal polynomial $g(x)$ of $f(\alpha, \gamma)$ is irreducible* mod p. *If*

$$\prod_{j=1}^{n} \prod_{i=1}^{m} [x - f(\alpha_i, \gamma_j)] \equiv [g(x)]^K \bmod p$$

for some K in I^+, then $f(\beta, \delta) \equiv f(\alpha, \gamma) \bmod p$.

PROOF. Denote by $a(x)$, $b(x)$, $c(x)$, $d(x)$ the minimal polynomials of $\alpha, \beta, \gamma, \delta$, respectively. Write $[b(x)]^M \equiv [a(x)]^{M'} \bmod p$ and $[d(x)]^N \equiv [c(x)]^{N'} \bmod p$, in accord with Definition 1. By Theorem 1,

$$(3) \quad \prod_j \prod_i [x - f(\beta_i, \delta_j)]^{MN} \equiv \prod_j \prod_i [x - f(\alpha_i, \gamma_j)]^{M'N'} \bmod p$$

where the α_i, β_i, γ_j, δ_j range through the conjugates of $\alpha, \beta, \gamma, \delta$. (We are not assuming here that α and β, nor γ and δ, have the same degree, only that the degrees of α and β divide r and those of γ and δ divide s.) By hypothesis the right side of (3) is $\equiv [g(x)]^{KM'N'} \bmod p$. The minimal polynomial of $f(\beta, \delta)$ is a factor of the left side of (3). By Lemma 3a, this polynomial is $\equiv [g(x)]^L$ for some L in I^+. By Definition 1, $f(\beta, \delta) \equiv f(\alpha, \gamma) \bmod p$.

DEFINITION 3. $b(x)$ *splits completely* $\bmod p$ if there exist rational integers $b_1, \cdots, b_n$, not necessarily distinct, such that

$$b(x) \equiv (x - b_1) \cdots (x - b_n) \bmod p.$$

Let $\mathcal{J}_p$ denote the set of β which are roots of such $b(x)$.

It is known that each $b(x)$ splits completely for infinitely many p. In fact, for any $a(x)$ and $b(x)$, infinitely many primes split both $a(x)$ and $b(x)$ completely. See [3] for *elementary* proofs.

COROLLARY 3a. *Under ordinary* $+$ *and* $\cdot$, $\mathcal{J}_p$ *is a ring.*

PROOF. Apply Lemma 3a to (1).

DEFINITION 4. Let $\mathcal{I}_p$ be the set of algebraic integers β such that $\beta \equiv c \bmod p$ for some c in I^+.

COROLLARY 3b. *Under ordinary* $+$ *and* $\cdot$, $\mathcal{I}_p$ *is a ring.*

PROOF. Apply Lemma 3a to (1).

EXAMPLE. Every second degree algebraic integer lies in an $\mathcal{I}_p$. Suppose $b(x) = x^2 + bx + a \in I[x]$. If b and a are both even then $b(x) \equiv x^2 \bmod 2$. If only b is even then $b(x) \equiv (x - 1)^2 \bmod 2$. Otherwise,

$$x^2 + bx + a \equiv \left(x - \frac{b^2 - 4a - b}{2}\right)^2 \bmod (b^2 - 4a).$$

THEOREM 4. *Suppose* $b(x)$ *splits completely* $\bmod p$. *Let* $q(x)$ *be the minimal polynomial of any coefficient in any monic polynomial which divides* $b(x)$ *over the complex number field. Then* $q(x)$ *splits completely* $\bmod p$.

PROOF. Any monic polynomial dividing $b(x) = \prod_{i=1}^{n} (x - \beta_i)$ has the form $a(x) = \prod_{k=1}^{m} (x - \beta_{i_k})$ with coefficients of the form $\sigma(\beta_{i_1}, \beta_{i_2}, \cdots, \beta_{i_m})$, where σ is an elementary symmetric function in m indeterminants.

For any m-element set $S = \{x_1, \cdots, x_m\}$ let S' denote the ordered m-tuple $(x_1, \cdots, x_m)$. Let $Q(x) = \prod [x - \sigma(S')]$, where S ranges through the m-element subsets of $\{\beta_1, \cdots, \beta_n\}$ (with repeated β's counted as distinct elements). The coefficients of $Q(x)$ are symmetric in $\beta_1, \cdots, \beta_n$, so $Q(x)$ has integer coefficients. In fact, each coefficient is a polynomial in the elementary symmetric functions of $\beta_1, \cdots, \beta_n$, and these were assumed congruent to corresponding coefficients in $\prod_{i=1}^{n} (x - b_i)$. Thus

$$Q(x) \equiv \prod [x - \sigma(s')] \mod p$$

where as above, s' ranges through m-tuples of b_i's. Each $\sigma(s')$ is an integer, so $Q(x)$ splits completely. Since $q(x)$ divides $Q(x) \bmod p$, Lemma 3a applies, and $q(x)$ must split completely mod p.

COROLLARY 4a. *Suppose $B(x) \equiv (x - b)^n \bmod p$ where $b \in I$, and suppose $A(x)$ is a monic polynomial of degree m with complex coefficients which divides $B(x)$ over the complex number field. Then $A(x) \equiv (x - b)^m \bmod p$, in the sense that the (not necessarily real) coefficients of $A(x)$ are respectively congruent as in Definition 2 to those of $(x - b)^m$.*

PROOF. First suppose $b = 0$. As in the proof of Theorem 4, we easily find $A(x) \equiv x^m$. Now for arbitrary b in 1, we have $B(x + b) \equiv x^n$ and $A(x + b)$ dividing $B(x + b)$. Thus $A(x + b) \equiv x^m$, so $A(x) \equiv (x - b)^m$.

The following generalization of Fermat's theorem shows that if $\beta \in \mathcal{J}_p$ and $b(0) \not\equiv 0 \bmod p$, then $\beta^{p-1} \in \mathcal{I}_p$.

THEOREM 5. *If $\beta \in \mathcal{J}_p$ and $b(0) \not\equiv 0 \bmod p$, then $\beta^{p-1} \equiv 1 \bmod p$.*

PROOF. Applying Theorem 2 to

$$\prod_{i=1}^{m} (x - \beta_i) \equiv \prod_{i=1}^{m} (x - r_i) \bmod p$$

gives

$$\prod_{i=1}^{m} (x - \beta_i^{p-1}) \equiv \prod_{i=1}^{m} (x - r_i^{p-1}) \bmod p$$

$$\equiv (x - 1)^m \bmod p.$$

By Lemma 3a, the minimal polynomial of β^{p-1} is congruent mod p to $(x-1)^s$ for some s in I^+.

Clearly if the restriction $b(0) \not\equiv 0$ is removed, then $b(x) \equiv x^r(x-1)^s$ for some r and s in I^+.

THEOREM 6. *Suppose α and β lie in $\mathcal{J}_p$. Let $f(x,y) \in I[x,y]$ and let d be the degree of $f(\alpha,\beta)$. If the prime p is less than d, then p divides the discriminant of $f(\alpha,\beta)$.*

PROOF. Let $g(x)$ denote the minimal polynomial of $f(\alpha,\beta)$. By Corollary 3*a*, there exist d integers g_i such that $0 \leqq g_i < p$ for $i = 1, 2, \cdots, d$, and

$$g(x) \equiv \prod_{i=1}^{d} (x - g_i) \bmod p.$$

Since $d > p$, we have $g_j = g_i$ for some $j \neq i$. As a symmetric function of the roots, the discriminant of $f(\alpha,\beta)$ is congruent mod p to that of the g_i's, which because of the repetition is congruent mod p to 0 (e.g., [5], p. 86).

REFERENCES

1. R. Bellman, *Introduction to Matrix Analysis*, McGraw-Hill, New York, 1970.
2. L. E. Dickson, *History of the Theory of Numbers*, v. 1, Chelsea, New York, 1951.
3. I. Gerst and J. Brillhart, *On the prime divisors of polynomials*, Amer. Math. Monthly **78** (1971), 250-266.
4. W. J. Guerrier, *The factorization of the cyclotomic polynomial mod p*, Amer. Math. Monthly **75** (1968), 46.
5. T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1964.
6. H. Pollard, *The Theory of Algebraic Numbers*, Carcus Mathematical Monograph No. 9, Mathematical Association of America, 1965.
7. B. L. van der Waerden, *Modern Algebra*, Ungar, New York, 1953.

UNIVERSITY OF EVANSVILLE, EVANSVILLE, INDIANA 47702