Canad. Math. Bull. Vol. **16** (4), 1973

ON FACTORIZATION OF POLYNOMIALS MODULO n

BY
ROBERT GILMER

Let A be an ideal of the commutative ring R with identity. There is a canonical homomorphism ϕ_A from the polynomial ring $R[X]$ onto $(R/A)[X]$, obtained by reducing all coefficients modulo A. If $f \in R[X]$, then we say that f is *reducible* (*irreducible*) modulo A if $\phi_A(f)$ is reducible (irreducible) in $(R/A)[X]$. If f is monic and is reducible in $R[X]$, then f is reducible modulo A for each nonzero proper ideal A of R, for f can be written as $g \cdot h$, where g and h are monic polynomials in $R[X]$ of positive degree. Hence $\phi_A(f)=\phi_A(g) \cdot \phi_A(h)$, where $\phi_A(g)$ and $\phi_A(h)$ are monic of positive degree, and consequently, are nonunits of $(R/A)[X]$(1). The purpose of this note is to prove that the converse of the preceding statement is false, even for the ring Z of integers. For example, Φ_{39}, the 39*th* cyclotomic polynomial, is reducible modulo n for each positive integer n, but Φ_{39} is irreducible in $Z[X]$. This statement will follow from more general considerations.

LEMMA 1. *Assume that $\{A_i\}_{i=1}^n$ is a finite set of pairwise comaximal ideals of the commutative ring R with identity, and that $f \in R[X]$ is reducible modulo A_i for each i between* 1 *and n. Then f is reducible modulo $A_1A_2 \cdots A_n$.*

Proof. By induction, it suffices to prove the lemma in the case where $n=2$. Thus we choose polynomials $h_1, h_2, g_1, g_2 \in R[X]$ such that

$$f \equiv g_i h_i (\text{mod } A_i), \quad \text{where} \quad \phi_{A_i}(g_i) \quad \text{and} \quad \phi_{A_i}(h_i)$$

are nonunits modulo A_i. Since the ideals A_1 and A_2 are comaximal, there exist polynomials $g, h \in R[X]$ such that

$$g \equiv g_i (\text{mod } A_i) \qquad h \equiv h_i (\text{mod } A_i).$$

Therefore, $f-gh \in A_1[X] \cap A_2[X]=(A_1 \cap A_2)[X]=(A_1A_2)[X]$. Moreover, if g or h were a unit modulo A_1A_2, this would contradict the fact that g_i and h_i are nonunits modulo A_i. Consequently, f is reducible modulo A_1A_2.

Received by the editors November 17, 1971 and, in revised form, March 22, 1972.

(1) If $f \in S[\{X_\lambda\}]$, where S is a commutative ring with identity and $\{X_\lambda\}$ is a set of indeterminates over S, then f is a unit of $S[\{X_\lambda\}]$ if and only if the constant term of f is a unit of S and each other coefficient of f is nilpotent [5].

https://doi.org/10.4153/CMB-1973-085-5 Published online by Cambridge University Press

THEOREM 1. *If $f \in Z[X]$ is a monic polynomial of positive degree, and if f has at least two nonassociate irreducible divisors modulo p for each prime p, then f is reducible modulo n for each positive integer n.*

Proof. By Lemma 1, it suffices to prove that f is reducible modulo p^k for each prime p and each positive integer k. By assumption, there are monic polynomials $g, h \in Z[X]$ of positive degree such that $f \equiv gh \pmod{p}$, where g and h are relatively prime modulo p. If A_p is the ring of p-adic integers, it follows that $f \equiv gh \pmod{pA_p}$, and Hensel's lemma [4, p. 185] implies that there are monic polynomials $g_1, h_1 \in A_p[X]$ such that $f = g_1h_1$, $\deg g_1 = \deg g$, $\deg h_1 = \deg h$, $g_1 \equiv g \pmod{pA_p}$, and $h_1 \equiv h \pmod{pA_p}$. Hence $f \equiv g_1h_1(p^kA_p)$ for each positive integer k, and since $A_p/p^kA_p \simeq Z/p^kZ$ [2, p. 224], it follows that there are polynomials $g_2, h_2 \in Z[X]$ such that $g_2 \equiv g_1(p^kA_p)$, $h_2 \equiv h_1(p^kA_p)$, $\deg g_2 = \deg g_1$, $\deg h_2 = \deg h_1$, and $f \equiv g_2h_2 \pmod{p^k}$. Therefore, f is reducible modulo p^k, and our proof is complete.

REMARK. In Theorem 1, it is easy to give a direct proof, without invoking Hensel's lemma, that f is reducible modulo p^k for each positive integer k (cf. [7, p. 205]). Thus if we assume, by induction, that $f \equiv g_{k-1}h_{k-1} \pmod{p^{k-1}}$, where $g_{k-1} \equiv g \pmod{p}$ and $h_{k-1} \equiv h \pmod{p}$, then we prove the existence of polynomials $r, s \in Z[X]$ such that if $g_k = g_{k-1} + p^{k-1}r$ and $h_k = h_{k-1} + p^{k-1}s$, then $f \equiv g_kh_k \pmod{p^k}$, $g_k \equiv g \pmod{p}$, and $h_k \equiv h \pmod{p}$. We let $f - g_{k-1}h_{k-1} = p^{k-1}t$, where $t \in Z[X]$. Then modulo p^k, $f - g_kh_k \equiv f - (g_{k-1} + p^{k-1}r)(h_{k-1} + p^{k-1}s) \equiv (t - rh_{k-1} - sg_{k-1})p^{k-1}$. If $u, v \in Z[X]$ are such that $ug_{k-1} + vh_{k-1} \equiv 1 \pmod{p}$, then $t - (tv)h_{k-1} - (tu)g_{k-1} \equiv 0 \pmod{p}$. Hence, if we take $r = tv$, $s = tu$, and we define $g_k = g_{k-1} + p^{k-1}r$ and $h_k = h_{k-1} + p^{k-1}s$, then g_k and h_k have the desired properties.

By means of Theorem 1, we can give examples of monic polynomials $f \in Z[X]$ such that f is reducible modulo n for each positive integer $n > 1$, while f is irreducible in $Z[X]$. A case of special interest here is that of the cyclotomic polynomials Φ_k. The factorization of Φ_k modulo p, for p prime, is known [3, p. 512], [1]. In fact, the following is true.

If $(p, k) = 1$, then Φ_k factors modulo p into a product of $\phi(k)/r$ nonassociate irreducible polynomials, each of degree r, where r is the order of p modulo k. If $(p, k) \neq 1$ and if $k = p^m s$, where $(s, p) = 1$, then modulo p, $\Phi_k = \Phi_s^{\phi(p^m)}$.

In particular, Φ_k is irreducible modulo some prime p if and only if the multiplicative group of units of $Z/(k)$ is cyclic(2). Therefore, Φ_{39} is reducible modulo p for each prime p, and since Φ_{39} is separable modulo p for each $p \neq 3, 13$, it follows that Φ_{39} has at least two irreducible prime divisors modulo p if $p \neq 3$ or 13. Moreover, 13 has order 1 modulo 3 and 3 has order 3 modulo 13, so that Φ_{39} factors modulo

(2) If n is a positive integer greater than one, then the multiplicative group of units of $Z/(n)$ is cyclic if and only if $n = 2, 4, p^t$, or $2p^t$ for some odd prime p [6, p. 92].

https://doi.org/10.4153/CMB-1973-085-5 Published online by Cambridge University Press

13 as $(X-3)^{12}(X-9)^{12}$, and modulo 3 as $f_1^2f_2^2f_3^2f_4^2$, where the f_i are distinct irreducible polynomials modulo 3 of degree 3. Hence, Theorem 1 implies that Φ_{39} is reducible modulo n for each positive integer n(3).

References

1. W. J. Guerrier, *The factorization of the cyclotomic polynomials mod p*, Amer. Math. Monthly **75** (1968), p. 46.
2. N. Jacobson, *Lectures in abstract algebra*, Vol. 3, Van Nostrand, Princeton, N.J., 1964.
3. L. Redei, *Algebra*, Vol. 1, Pergamon Press, New York, 1967.
4. P. Ribenboim, *Théorie des valuations*, Univ. of Montreal Press, Montreal, 1964.
5. E. Snapper, *Completely primary rings*, Ann. of Math. (2) **52** (1950), 666–693.
6. D. Shanks, *Solved and unsolved problems in number theory*, Spartan Books, Washington, D.C., 1962.
7. B. L. van der Waerden, *Algebra*, Vol. 2, Ungar, New York, 1970.

Florida State University,
Tallahassee, Florida

(3) Other integers k such that ϕ_k is reducible modulo n for each positive integer n are 55, 95, 111, 3^a13^b, 5^a11^b, 5^a19^b, and 3^a37^b for all positive integers a and b. On p. 408 of *History of the Theory of Numbers*, Volume II, L. E. Dickson remarks that the polynomial t^4+13t^2+81 is irreducible in $Z[t]$, but reducible modulo p^e for each prime p and each positive integer e.

https://doi.org/10.4153/CMB-1973-085-5 Published online by Cambridge University Press