DTIC FILE COPY

Naval Research Laboratory

Washington, DC 20375-5000

NRL Memorandum Report 6605

AD-A218 148

Euler's Theorem for Polynomials

WILLIAM WARDLAW

Identification Systems Branch
Radar Division

DTIC
ELECTE
FEB 2 2 1990
S D
D

February 9, 1990

Approved for public release; distribution unlimited.

90 02 21 015

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release, distribution unlimited.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) NRL Memorandum Report 6605	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Research Laboratory 6b. OFFICE SYMBOL (If applicable) Code 5350	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) Washington, DC 20375-5000	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION Naval Air Systems Command 8b. OFFICE SYMBOL (If applicable) APC-209C	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code) Washington, DC 20361	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. 64211N; PROJECT NO.; TASK NO.; WORK UNIT ACCESSION NO. DN180-248
11. TITLE (Include Security Classification) Euler's Theorem for Polynomials	
12. PERSONAL AUTHOR(S) Wardlaw, William P.	
13a. TYPE OF REPORT Final 13b. TIME COVERED FROM Aug 88 TO Aug 89	14. DATE OF REPORT (Year, Month, Day) 1990 February 9 15. PAGE COUNT 11
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Finite fields; Polynomials; Factorization of polynomials; Euler Totient Theorem

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

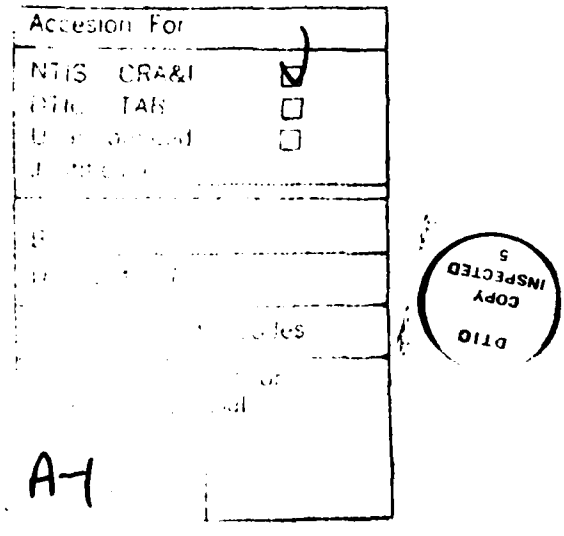
The similarity of the arithmetic of the integers and the arithmetic of polynomials suggests that an analog of Euler's Totient Theorem for integers also holds for polynomials over a finite field. This theorem is stated and proved, and then some properities of the totient function for polynomials are derived. The related notions of the order of one polynomials modulo another relatively prime polynomial, and of the exponent of a polynomial, are investigated. Finally, examples are given which show how to apply these ideas to the factorization of polynomials over finite fields.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Emanuel Vegh	22b. TELEPHONE (Include Area Code) 202 767-3481 22c. OFFICE SYMBOL Code 5350

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

CONTENTS



EULER'S THEOREM FOR POLYNOMIALS

INTRODUCTION

The similarity of the theory of divisibility for integers and that for polynomials is striking. For example, the Euclidean algorithm, the formula

(1) $$(a, b) = ca + db$$

for the greatest common divisor (a, b) of a and b, the arithmetic of elements modulo a fixed element m, and the criterion

(2) a is invertible modulo m iffi $(a, m) = 1$,

all apply equally well for integers, or for polynomials, a, b, c, d, and m. Both theories measure the distance of an element from zero, by the absolute value $|a|$ of an integer a, or by the degree ∂a of a polynomial a.

This similarity suggests a polynomial analogue to Euler's pretty theorem on modular arithmetic:

Euler's Theorem. If a and m are integers with $(a, m) = 1$ and $\phi(m) = |\{k \in \mathbb{Z} : 0 < k < |m|, (k, m) = 1\}|$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Such an analogue does indeed exist, and the analogy is almost exact! We begin the next section with a statement of this analogous theorem. We continue by discussing the related

Manuscript approved August 30, 1989.

concepts, the order of a polynomial f modulo a relatively prime polynomial m, and the exponent $\exp(m)$ of the polynomial m. We end with some applications of these ideas to the factorization of polynomials over finite fields. The factorization of polynomials over the two element field $GF(2)$ is important in the design of linear feedback shift registers.

EULER'S THEOREM FOR POLYNOMIALS

Theorem 1. (Euler's Theorem for Polynomials). Let $m \in K[x]$, where K is a finite field, and let

$$\varphi(m) = |\{f \in K[x] : 0 \leq \partial f < \partial m \text{ and } (f, m) = 1\}|.$$

Then for any $f \in K[x]$ with $(f, m) = 1$,

$$f^{\varphi(m)} \equiv 1 \pmod{m}. \tag{3}$$

Proof. Let $K_m = K[x]/(m)$. Then K_m is a ring and K_m^* is the group of invertible elements of K_m. $(f, m) = 1$ implies that $f_m = f + (m) \in K_m^*$. Since $|K_m^*| = \varphi(m)$, it follows by Lagrange's theorem that

$$f^{\varphi(m)} \equiv f_m^{\varphi(m)} \equiv 1 \pmod{m}. \blacksquare$$

It should come as no surprise that an immediate corollary is an analogue to Fermat's Little Theorem:

Corollary 1.1. (Fermat's Little Theorem for Polynomials) Let K be a field of q elements and let g be an irreducible polynomial over K of degree d. Then $f \in K[x]$ implies

$$f^{q^d} \equiv f \pmod{g}. \tag{4}$$

Proof. There are $r = q^d$ polynomials of degree $< d$ over K, one of which is 0, so $\varphi(g) = r - 1$, since g is irreducible. Thus, $f \not\equiv 0 \pmod{g}$ implies $(f, g) = 1$, so $f^{r-1} \equiv 1 \pmod{g}$ by (3), and multiplication by f gives (4). Otherwise, $g \mid f$, and (4) is clear. ∎

Note that taking $f = x$ in (4) shows that if g is an irreducible polynomial of degree d over a field K of q elements, then

$$g \mid x^{q^d} - x. \tag{5}$$

This result can be useful. For example, the negation of (5) can be used to show that g is reducible in $K[x]$. A different and somewhat (the author feels) more complicated derivation of (5) can be obtained using the properties of splitting fields and algebraic extensions of K. Then one can use the arithmetic in K (The facts needed are that $a^q = a$ and $(u + v)^q = u^q + v^q$ for $a \in K$ and $u, v \in K[x]$.) to show that $(f(x))^q = f(x^q)$, and then apply (5) to obtain (4).

One problem in using Theorem 1 is the evaluation of $\varphi(m)$. Analogy again saves the day: φ turns out to be multiplicative!

Theorem 2. Let K be a field with q elements and let $f, g \in K[x]$. Then:

a. $(f, g) = 1$ implies $\varphi(fg) = \varphi(f)\varphi(g)$.
b. $\varphi(f) \leq q^{\partial f} - 1$.
c. g irreducible iffi $\varphi(g) = q^{\partial g} - 1$.
d. g irreducible, $k \in \mathbb{N}$, and $r = q^{\partial g}$ implies

$$\varphi(g^k) = (r - 1)r^{k-1}.$$

Proof. a. (This proof is an exact analogue of the author's favorite proof of the multiplicative property of the arithmetic totient function. One only needs to replace $Z_n = Z/(n)$ by K_f.) As before, denote $K_f = K[x]/(f)$ and $h_f = h + (f)$. For any $f, g \in K[x]$, $\alpha : K_{fg} \to K_f \oplus K_g : h_{fg} \to (h_f, h_g)$ is a homomorphism into $K_f \oplus K_g$. h_{fg} is in the kernel iffi $f \mid h$ and $g \mid h$. Therefore, $(f, g) = 1$ implies $\ker \alpha = \{0\}$, so $K_{fg} \cong K_f \oplus K_g$, $K_{fg}^* \cong (K_f \oplus K_g)^* \cong K_f^* \times K_g^*$, and

$$\varphi(fg) = |K_{fg}^*| = |K_f^*||K_g^*| = \varphi(f)\varphi(g),$$

as claimed.

b. $\varphi(f) = |K_f^*| \leq |K_f| - 1 = q^{\partial f} - 1$ since $K_f^* \subseteq K_f \setminus \{0\}$.

c. g irreducible iffi $K_g^* = K_g \setminus \{0\}$ iffi $\varphi(g) = q^{\partial g} - 1$.

d. The polynomial g^k has degree dk, where $d = \partial g$ is the degree of g. There are q^{dk} polynomials in $K[x]$ with degree $< dk$, and $q^{d(k-1)}$ of these are divisible by g. Thus, if g is irreducible and $r = q^d$,

$$\varphi(g^k) = q^{dk} - q^{d(k-1)} = r^k - r^{k-1}. \blacksquare$$

THE ORDER OF f MODULO m

For relatively prime polynomials f and m over a finite field K, define the order of f modulo m to be the number

$$(6) \qquad o_m(f) = \min(n \in \mathbf{N} : f^n \equiv 1 \pmod m).$$

This number exists by Theorem 1.

Theorem 3. If K is a finite field, $f, g, h \in K[x]$, and $(fg, h) = 1$, then:

a. $f \mid g$ implies $o_f(h) \mid o_g(h) \mid \varphi(g)$.

b. $(f, g) = 1$ implies that $o_{fg}(h) = \text{lcm}[o_f(h), o_g(h)]$.

Proof. a. Since $o_g(h)$ is the order of the element h_g in the group K_g^*, it is clear that $o_g(h) \mid \varphi(g) = |K_g^*|$. Now, $o_g(h) = n$ implies that g divides $h^n - 1$, and so f does, also. Thence $h^n \equiv 1 \pmod f$ and $o_f(h) \mid n = o_g(h)$.

b. Since $(f, g) = 1$, $K_{fg}^* \cong K_f^* \times K_g^*$, as shown in the proof of Theorem 2. Hence, $o_{fg}(h)$ is the order of h_{fg} in K_{fg}^*, which is the order of its isomorphic image (h_f, h_g) in $K_f^* \times K_g^*$. The latter is clearly $\text{lcm}[o_f(h), o_g(h)]$.■

THE EXPONENT OF A POLYNOMIAL

We conclude with some applications of the above. The exponent of a polynomial f is defined to be the number

$$\exp(f) = \min\{n \in \mathbf{N} : f \mid x^n - 1\}, \tag{7}$$

or $\exp(f) = 0$ if the set on the right hand side is empty. Since $f(0) \neq 0$ iffi $(f, x) = 1$, comparison of (6) and (7) shows that over a finite field,

$$\exp(f) = o_f(x) > 0 \text{ iffi } f(0) \neq 0. \tag{8}$$

The exponent of a polynomial over $K = GF(2)$ is of importance in constructing linear shift register sequences. (See [G].) After proving the next theorem, we will see that it is also useful in factoring, or determining the irreducibility, of a polynomial.

Theorem 4. Let K be a field of characteristic p which has q elements, and let $f, g \in K[x]$ with $g(0) \neq 0$. Then:

a. $f(0) = 0$ iffi $\exp(f) = 0$.

b. $f \mid g$ implies $\exp(f) \mid \exp(g) \mid \varphi(g)$.

c. $\partial g \leq \exp(g) \leq q^{\partial g} - 1$.

d. $(f, g) = 1$ implies $\exp(fg) = \text{lcm}[\exp(f), \exp(g)]$.

e. g irreducible implies $\exp(g) \mid q^{\partial g} - 1$.

f. g irreducible implies $\exp(g^k) = p^r \exp(g)$, where k and r are positive integers such that $p^{r-1} < k \leq p^r$.

g. $\exp(g) = q^{\partial g} - 1$ implies g is irreducible.

h. g has repeated irreducible factors iffi $p \mid \exp(g)$.

Proof. a. The result is immediate from (8).

b. The result follows from (8) by taking $h = x$ in Theorem 3.a.

c. $\partial g \leq \exp(g)$ since $g \mid x^{\exp(g)} - 1$, and $\exp(g) \leq \varphi(g) \leq q^{\partial g} - 1$ by b. and Theorem 2.b.

d. If $f(0) = 0$, both sides of the equation give 0. Otherwise, the result follows from (8) and Theorem 3.b. with $h = x$.

e, g. The results are immediate from b. and Theorem 2.b,c.

f. Let $e = \exp(g)$. Then $g \mid x^e - 1$ implies that $g \mid g^k \mid (x^e - 1)^k \mid (x^e - 1)^{p^r} = x^{ep^r} - 1$, so $\exp(g) = e \mid \exp(g^k) \mid \exp(x^{ep^r} - 1) = ep^r$, by part b. Hence, $\exp(g^k) = ep^s$ with $0 \leq s \leq r$. Now $(e, q) = 1$ by part e., so $(e, p) = 1$ (since q is a power of p) and $x^e - 1$ has no repeated roots follows from the fact that $x^e - 1$ and its formal derivative ex^{e-1} are relatively prime in K. It follows that $g^k \mid x^{ep^s} - 1 = (x^e - 1)^{p^s}$ only if $p^s \geq k$; i.e., $s = r$ and $\exp(g^k) = ep^r$.

h. The result follows by d, f, and the proof of f.■

APPLICATIONS TO FACTORING

Example 1. Let $K = GF(2)$ and $f = x^7 + x + 1$. Taking congruences modulo f, $x^7 \equiv x + 1$, $x^8 \equiv x^2 + x$, $x^{56} = (x^7)^8 \equiv (x + 1)^8 = x^8 + 1 \equiv x^2 + x + 1$, $x^{112} = (x^{56})^2 \equiv (x^2 + x + 1)^2 = x^4 + x^2 + 1$, $x^{16} = (x^8)^2 \equiv (x^2 + x)^2 = x^4 + x^2$, $x^{15} \equiv x^3 + x$, so $x^{127} = (x^{15})(x^{112}) \equiv (x^3 + x)(x^4 + x^2 + 1) = x^7 + x \equiv 1$. Hence, $\exp(f) \mid 127$, so $\exp(f) = 127 = 2^7 - 1$ and f is irreducible by Theorem 4.g.

Example 2. Let $K = GF(2)$ and $g = x^7 + x^6 + x^2 + x + 1$. Take congruences modulo g for x^k with $k = 7, 8, 9, 10, 12, 20$, and 19 to show $x^9 \equiv (x + 1)^6$ and $x^{19} \equiv x + 1$. Thus $x^{114} \equiv (x^{19})^6 \equiv x^9$ and $x^{105} \equiv 1$, but $x^k \not\equiv 1$ for $k = 35, 21$, and 15 since $x^{38} \not\equiv x^3$, $x^{21} \not\equiv 1$, and $x^{19} \not\equiv x^4$. Therefore, $\exp(g) = 105 = 3 \cdot 5 \cdot 7$.

Since $g(0) = g(1) = 1$, g has no linear factor, and hence has no irreducible factor of degree 6. For $d = 2, 3, 4, 5$, or 7, Theorem 4.e. shows that the exponent of an irreducible factor of degree d must divide $2^d - 1 = 3, 7, 15, 31$, or 127 respectively. In view of Theorem 4.e., the factors 7 and 5 of $\exp(g)$ imply g has irreducible factors of degrees $d = 3$ and $d = 4$, respectively. Now $x^3 + x + 1$ and $x^3 + x^2 + 1$ are the only irreducible cubics over $K = GF(2)$: The others all have a linear factor. Knowing this, it is easy to factor

$$g = x^7 + x^6 + x^2 + x + 1 = (x^3 + x^2 + 1)(x^4 + x + 1).$$

Example 3. Let $K = GF(2)$ and $h = x^7 + x^4 + x^2 + x + 1$. The reader can verify that $\exp(h) = 42$. Thus h has a repeated irreducible factor by Theorem 4.h. The formal derivative of h

is $h' = x^6 + 1$, and the Euclidean algorithm gives

$$(h, h') = x^4 + x^2 + 1 = (x^2 + x + 1)^2.$$

From this it is easy to find the factorization

$$h = (x^2 + x + 1)^2(x^3 + x + 1).$$

Example 4. Consider the cyclotomic polynomials $c_5 = x^4 + x^3 + x^2 + x + 1$ and $c_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ over $K = GF(2)$. $\exp(c_5) = 5 \mid 2^4 - 1$ but does not divide $2^d - 1$ for $1 < d < 4$, so c_5 is irreducible. $\exp(c_7) = 7 \mid 2^6 - 1$, but $7 \mid 2^3 - 1$ also, so c_7 can have a factor of degree 3. In fact, $c_7 = (x^3 + x + 1)(x^3 + x^2 + 1)$. These examples show that "implies" cannot be replaced by "iffi" in Theorem 4.e or g.

CONCLUSION

Euler's Theorem for Polynomials is completely analogous to the corresponding theorem for integers, and it provides a powerful tool for examining the powers of a polynomial modulo another polynomial over a finite field. Theorem 3 gives an easy method for evaluating $\varphi(m)$ for any polynomial $m(x)$, once $m(x)$ is given as a product of powers of its irreducible factors.

More importantly, knowledge of $\varphi(m)$ gives considerable information about the factorization of $m(x)$. The related concepts of the order, $o_m(f)$, of a polynomial f modulo the polynomial m, and the exponent, $\exp(m)$, of m, give an organized method of factoring a polynomial $m(x)$ over a finite field. The ease of calculating $\exp(m)$ makes Theorem 4 especi-

ally useful for factoring.

The factorization of polynomials over finite fields is important in coding theory and the design of linear feedback shift registers. For the latter, one especially wants to find polynomials over the two element field, GF(2), which are irreducible of prime degree p such that $L = 2^p - 1$ is a Mersenne prime. (See the corollary to Theorem 3.1 in [G], p. 37, or Corollary 7 in [W], p. 13.) The examples in the preceding section show how Theorem 4 applies particularly well to this situation.

REFERENCES

[G] Solomon W. Golomb, Shift Register Sequences, rev. ed., Aegean Park Press, Laguna Hills, CA. (1982).

[W] William P. Wardlaw, A Matrix Model for the Linear Feedback Shift Register, NRL Report 9179, Naval Research Laboratory, Washington, DC 20375-5000 (1989)