The Arithmetic of Polynomials Modulo p

In §§1,2, proofs are to be supplied by the reader, results under discussion are analogous to those in the NZM text, and the numbering is intended to emphasize the correspondence. One may view this unit as an introduction to finite fields, but in a very old-fashioned way, from the viewpoint of classical elementary number theory.

Throughout, p is a fixed prime. Suppose that $f(x) = \sum a_i x^i$ and $g(x) = \sum b_i x^i$ are two polynomials. We must distinguish between the following two assertions:

(I) $a_i \equiv b_i \pmod p$ for all i;

(II) $f(x) \equiv g(x) \pmod p$ for all integers x.

Of course (I) implies (II) but the converse is false (since for example we might have $f(x) = x^p - x$ and $g(x) = 0$). To facilitate this distinction we adopt a notation that is consistent with modern algebra. We let F_p denote the field of residue classes modulo p, and $F_p[x]$ the ring of polynomials whose coefficients are residue classes (mod p). We write $f(x) = g(x)$, or more briefly $f = g$ if (I) holds.

1. Divisibility and Factorization

The theory here is entirely analogous to the theory we have developed for the integers. The numbering below coincides with that in NZM, and the proofs are parallel. Hence, we hold these truths to be self-evident:

Definition 1.1. *If $f \in F_p[x]$ and $g \in F_p[x]$ then we say that f* divides *g, and write $f|g$, if there is a polynomial $m \in F_p[x]$ such that $mf = g$. We say that f and g are* associates *if there is a non-zero residue class $c \in F_p^\times$ such that $cf = g$.*

Theorem 1.1. *Suppose that a, b, c are polynomials in $F_p[x]$. Then*
(1) *$a|b$ implies that $a|bc$ for any $c \in F_p[x]$;*
(2) *$a|b$ and $b|c$ imply that $a|c$;*
(3) *$a|b$ and $a|c$ imply that $a|(bu + cv)$ for any $u, v \in F_p[x]$;*
(4) *If $a|b$ then $\deg a \le \deg b$.*
(5) *$a|b$ and $b|a$ imply that a and b are associates.*
(6) *Suppose that m is a non-zero polynomial in $F_p[x]$. Then $a|b$ if and only if $ma|mb$.*

Theorem 1.2. (The division algorithm) *Let a and b be polynomials in $F_p[x]$ with $a \ne 0$. Then there exist polynomials q and r in $F_p[x]$ such that $b = qa + r$ and $\deg r < \deg a$.*

The remainder r may be 0 (the zero polynomial, all of whose coefficients are 0); we put $\deg 0 = -\infty$. Thus the identity $\deg ab = \deg a + \deg b$ holds even when one of the factors is 0.

Definition 1.2. *Let a and b be polynomials in $F_p[x]$. We say that a polynomial $d \in F_p[x]$ is a* common divisor *of a and b if $d|a$ and $d|b$. If $a \neq 0$ or $b \neq 0$ then we say that $g \in F_p[x]$ is a* greatest common divisor *of a and b if g is a common divisor of a and b and $\deg g$ is maximal among all common divisors of a and b. In this case we write $g = (a, b)$.*

Theorem 1.3. *If $g \in F_p[x]$ is a greatest common divisor of b and c then there exist polynomials u and v in $F_p[x]$ such that $g = bu + cv$. Any two greatest common divisors of b and c are associates.*

Theorem 1.4. *The greatest common divisor g of two polynomials b and c in $F_p[x]$ can be characterized in the following two ways:* (1) *Among non-zero polynomials of the form $bu + cv$ where u and v are polynomials in $F_p[x]$, g has minimal degree;* (2) *g is a common divisor of b and c that is divisible by every other common divisor.*

Theorem 1.5. *Given any polynomials $b_1, b_2, \ldots, b_n$ in $F_p[x]$, not all zero, with greatest common divisor g, there exist polynomials $u_1, u_2, \ldots, u_n$ such that*

$$g = (b_1, b_2, \ldots, b_n) = \sum_{j=1}^{n} b_j u_j.$$

Among all non-zero polynomials of the form $\sum_{j=1}^{n} b_j v_j$, where the v_j are polynomials in $F_p[x]$, g is one whose degree is minimal. All common divisors of $b_1, b_2, \ldots, b_n$ divide g, and any two greatest common divisors are associates.

Theorem 1.6. *If a and b are polynomials in $F_p[x]$, not both zero, and if m is a non-zero polynomial in $F_p[x]$, then $(ma, mb) = m(a, b)$.*

Theorem 1.7. *Suppose that a and b are polynomials in $F_p[x]$, not both zero. If d is a non-zero polynomial in $F_p[x]$ such that $d|a$ and $d|b$, then*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b).$$

In particular, if $g = (a, b)$ then

$$\left(\frac{a}{g}, \frac{b}{g}\right) = 1.$$

Theorem 1.8. *Let a, b, and m be polynomials in $F_p[x]$, at least two of them non-zero. If $(a, m) = 1$ and $(b, m) = 1$, then $(ab, m) = 1$.*

Definition 1.3. *Let a and b be polynomials in $F_p[x]$. We say that a and b are* relatively prime *if $(a, b) = 1$. We say that $a_1, a_2, \ldots, a_n$ are* relatively prime *if $(a_1, a_2, \ldots, a_n) = 1$. We say that $a_1, a_2, \ldots, a_n$ are* relatively prime in pairs *if $(a_i, a_j) = 1$ for all $i = 1, 2, \ldots, n$ and all $j = 1, 2, \ldots, n$ with $j \neq i$.*

Theorem 1.9. *Let a and b be polynomials in $F_p[x]$, not both zero, and let x be any polynomial in $F_p[x]$. Let c be any non-zero residue class* (mod p)*. Then $(a,b)=(b,a)=(a,cb)=(a,b+ax)$.*

Theorem 1.10. *Suppose that a, b, and c are polynomials in $F_p[x]$. If $c|ab$ and $(b,c)=1$, then $c|a$.*

Theorem 1.11. (The Euclidean Algorithm) *Given polynomials b and $c\neq 0$ in $F_p[x]$, we make a repeated application of the division algorithm, Theorem 1.2, to obtain a series of equations*

$$
\begin{aligned}
b &= cq_1 + r_1, & 0 &< \deg r_1 < \deg c,\\
c &= r_1q_2 + r_2 & 0 &< \deg r_2 < \deg r_1,\\
r_1 &= r_2q_3 + r_3, & 0 &< \deg r_3 < \deg r_2,\\
&\ \ \vdots & &\ \ \vdots\\
r_{j-2} &= r_{j-1}q_j + r_j & 0 &< \deg r_j < \deg r_{j-1},\\
r_{j-1} &= r_jq_{j+1}.
\end{aligned}
$$

The greatest common divisor (b,c) of b and c is r_j, the last non-zero remainder in the division process. Values of u_0 and v_0 in $(b,c)=bu_0+cv_0$ can be obtained by writing each r_i as a linear combination of b and c.

Definition 1.4. *The polynomials $a_1,a_2,\dots,a_n$ in $F_p[x]$, all different from zero, have a* common multiple *b if $a_i|b$ for all $i=1,2,\dots,n$. (Note that common multiples do exist; for example the product $a_1a_2\cdots a_n$ is one.) The* least common multiple *of the a_i is non-zero common multiple of minimal degree, and is denoted by $[a_1,a_2,\dots,a_n]$.*

Theorem 1.12. *If b is a common multiple of the polynomials $a_1,a_2,\dots,a_n$ in $F_p[x]$ then $[a_1,a_2,\dots,a_n]|b$. This is the same thing as saying that if $h=[a_1,a_2,\dots,a_n]$ then the common multiples of the a_i are precisely the polynomials of the form mh where m ranges over all polynomials in $F_p[x]$.*

Theorem 1.13. *If m, a, and b are non-zero polynomials in $F_p[x]$ then $[ma,mb]=m[a,b]$. Also, $[a,b](a,b)=ab$.*

Definition 1.5. *A polynomial $f\in F_p[x]$ is called* reducible *if it can be written in the form $f=ab$ where a and b are non-constant polynomials. If f has no divisor d satisfying $0<\deg d<\deg f$ then f is* irreducible.

Theorem 1.14. *Every non-constant polynomial $a\in F_p[x]$ can be written as a product of irreducible polynomials.*

Theorem 1.15. *Suppose that f, a, and b are non-zero polynomials in $F_p[x]$. If f is irreducible and $f|ab$ then $f|a$ or $f|b$. More generally, if $f|a_1a_2\cdots a_n$ then $f|a_i$ for at least one $i=1,2,\dots,n$.*

Theorem 1.16. (The Fundamental Theorem of Arithmetic) *The factoring of a polynomial $a \in F_p[x]$ into irreducible polynomials is unique apart from the ordering of the factors, and the choice of associates.*

Suppose that a, b, c are polynomials in $F_p[x]$ with factorizations

$$a = \prod_f f^{\alpha(f)} \qquad\qquad b = \prod_f f^{\beta(f)} \qquad\qquad c = \prod_f f^{\gamma(f)}$$

where the polynomials f are irreducible. If $ab = c$ then by Theorem 1.16 we deduce that $\alpha(f) + \beta(f) = \gamma(f)$ for all f. Hence $a|c$ if and only if $\alpha(f) \le \gamma(f)$ for all irreducible polynomials $f \in F_p[x]$. Consequently, the greatest common divisor and least common multiple of a and b have factorizations

$$(a, b) = \prod_f f^{\min(\alpha(f),\beta(f))}, \qquad\qquad [a, b] = \prod_f f^{\max(\alpha(f),\beta(f))}.$$

Thus the identity of Theorem 1.6 is equivalent to the identity $\min(\mu+\alpha, \mu+\beta) = \mu + \min(\alpha, \beta)$, and the second identity in Theorem 1.13 is equivalent to the identity $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$.

The results here do not depend on the fact that the ground field is the field F_p of residues modulo p. Thus in abstract algebra, one proves that if F is an arbitrary field then the polynomials $F[x]$ with coefficients in F have a division algorithm, which yields a Euclidean algorithm, and hence unique factorization. Moreover, if I is an ideal in the ring $F[x]$, then by Theorem 1.5 we know that I is principal; that is, there is a polynomial $f \in F[x]$ such that $I = (f)$. This gives rise to a quotient ring $F[x]/(f)$, whose structure is also subject to investigation. In the case of $F_p[x]/(f)$ we develop this in the next section, using the more number-theoretic language of congruences.

2. Congruences

Definition 2.1. *Let m be a non-zero polynomial in $F_p[x]$. If a and b are polynomials in $F_p[x]$ such that $m|(a-b)$ then we say that a is* congruent to b modulo m, *and we write $a \equiv b \pmod{m}$. If $m \nmid (a-b)$ then we write $a \not\equiv b \pmod{m}$.*

Theorem 2.1. *Let a, b, c, and d denote polynomials in $F_p[x]$, and let f be a non-zero polynomial in $F_p[x]$. Then:*

(1) *$a \equiv b \pmod{f}$, $b \equiv a \pmod{f}$, and $a - b \equiv 0 \pmod{f}$ are equivalent statements;*
(2) *If $a \equiv b \pmod{f}$ and $b \equiv c \pmod{f}$ then $a \equiv c \pmod{f}$;*
(3) *If $a \equiv b \pmod{f}$ and $c \equiv d \pmod{f}$ then $a + c \equiv b + d \pmod{f}$;*
(4) *If $a \equiv b \pmod{f}$ and $c \equiv d \pmod{f}$ then $ac \equiv bd \pmod{f}$;*
(5) *If $a \equiv b \pmod{f}$ and $d|f$ then $a \equiv b \pmod{d}$;*
(6) *If $a \equiv b \pmod{f}$ then $ac \equiv bc \pmod{fc}$.*

Theorem 2.2. *Suppose that a, b, and f are polynomials in $F_p[x]$. If P is a polynomial in $F_p[x]$ and $a \equiv b \pmod{f}$ then $P(a) \equiv P(b) \pmod{f}$.*

Theorem 2.3. *Suppose that a, u, v, and f are polynomials in $F_p[x]$. Then*
(1) $au \equiv av \pmod{f}$ *if and only if* $u \equiv v \pmod{\frac{f}{(a,f)}}$.
(2) *If* $au \equiv av \pmod{f}$ *and* $(a, f) = 1$ *then* $u \equiv v \pmod{f}$.
(3) $u \equiv v \pmod{f_i}$ *for* $i = 1, 2, \ldots, r$ *if and only if* $u \equiv v \pmod{[f_1, f_2, \ldots, f_r]}$.

Definition 2.2. *Suppose that u, v, and f are polynomials in $F_p[x]$. If $u \equiv v \pmod{f}$ then we say that v is a* residue *of u modulo f. A set $u_1, u_2, \ldots, u_k$ is called a* complete residue system *modulo f if for every polynomial v in $F_p[x]$ there is one and only one u_i such that $v \equiv u_i \pmod{f}$.*

The set of polynomials of degree less than the degree of f form a complete system of residues modulo f. Hence the number of residues in a complete system is $k = p^{\deg f}$.

Theorem 2.4. *Suppose that b, c, and f are polynomials in $F_p[x]$. If $b \equiv c \pmod{f}$ then $(b, f) = (c, f)$.*

Definition 2.3. *Let f be a polynomial in $F_p[x]$. A* reduced residue system *modulo f is a set of polynomials $r_1, r_2, \ldots, r_k$ such that $(r_i, f) = 1$ and $r_i \not\equiv r_j \pmod{f}$ if $i \neq j$, and such that if u is a polynomial such that $(u, f) = 1$, then $u \equiv r_i \pmod{f}$ for exactly one value of i.*

If f is irreducible in $F_p[x]$, then all polynomials of degree less than that of f are relatively prime to f, except for the zero polynomial. Hence in this case the number of polynomials in a system of reduced residues is $p^{\deg f} - 1$.

Theorem 2.6. *Suppose that a and f are polynomials in $F_p[x]$, and that $(a, f) = 1$. Let $r_1, r_2, \ldots, r_k$ be a complete, or reduced, system of residues modulo f. Then $ar_1, ar_2, \ldots, ar_k$ is a complete, or reduced system of residues, respectively, modulo f.*

Theorem 2.7. *Let f be an irreducible polynomial in $F_p[x]$ of degree n. If $f \nmid a$ then $a^{p^n - 1} \equiv 1 \pmod{f}$.*

Theorem 2.8. *Let f be a polynomial in $F_p[x]$, and let $\phi(f)$ be the number of polynomials in a reduced system of residues modulo f. If $(a, f) = 1$ then $a^{\phi(f)} \equiv 1 \pmod{f}$.*

Theorem 2.9. *Let a and f be polynomials in $F_p[x]$. If $(a, f) = 1$ then there is a polynomial u such that $au \equiv 1 \pmod{f}$. Any two such u are congruent $\pmod{f}$. If (a, f) is a polynomial of degree > 0 then there is no such u.*

Theorem 2.10. *Let u and f be polynomials in $F_p[x]$, and suppose that f is irreducible. Then $u^2 \equiv 1 \pmod{f}$ if and only if $u \equiv \pm 1 \pmod{f}$.*

Theorem 2.11. *Let f be an irreducible polynomial in $F_p[x]$, and let $r_1, r_2, \ldots, r_k$ be a system of reduced residues modulo f. Then $\prod_{i=1}^{k} r_i \equiv -1 \pmod{f}$.*

Definition 2.4. *Let f be a polynomial in $F_p[x]$, and let $r_1, r_2, \ldots, r_k$ be a complete system of residues modulo f. Let $P(z)$ be a polynomial whose coefficients are in $F_p[x]$. The* number of solutions *of the congruence $P(u) \equiv 0 \pmod{f}$ is the number of i for which $P(r_i) \equiv 0 \pmod{f}$.*

Theorem 2.18. (The Chinese Remainder Theorem) *Let $f_1, f_2, \ldots, f_r$ be non-zero polynomials in $F_p[x]$, and suppose that the f_i are relatively prime in pairs. Let $a_2, a_2, \ldots, a_r$ be any polynomials in $F_p[x]$. Then there is a polynomial u such that $u \equiv a_i \pmod{f_i}$ for $i = 1, 2, \ldots r$. If $f = f_1 f_2 \cdots r_r$ then any two such u are congruent modulo f.*

Theorem 2.19. *If a is a polynomial in $F_p[x]$ let $\phi(a)$ be the number of polynomials in a reduced system of residues modulo a. If $(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$. If $a = \prod_f f^\alpha$ is the factorization of a into irreducible polynomials, then $\phi(a) = \prod_f p^{n(\alpha-1)}(p^n - 1)$ where $n = n_f = \deg f$.*

Theorem 2.20. *Let a and b denote polynomials in $F_p[x]$, and let $P(z)$ be a polynomial whose coefficients are in $F_p[x]$. Let $N_P(a)$ denote the number of solutions of the congruence $P(u) \equiv 0 \pmod{a}$. If $(a, b) = 1$ then $N_P(ab) = N_P(a)N_P(b)$.*

Theorem 2.26. *Let f be an irreducible polynomial in $F_p[x]$, and let $P(z)$ be a polynomial of degree k whose coefficients are in $F_p[x]$. Then the congruence $P(u) \equiv 0 \pmod{f}$ has at most k solutions.*

Theorem 2.29. *Let f be an irreducible polynomial in $F_p[x]$, and let $n = \deg f$. Suppose that $P(z)$ be a polynomial of degree k whose coefficients coefficients are in $F_p[x]$. Then the congruence $P(u) \equiv 0 \pmod{f}$ has exactly k solutions if and only if there is a polynomial $Q(z)$ whose coefficients are in $F_p[x]$ such that $u^{p^n} - u \equiv P(u)Q(u) \pmod{f}$ for all polynomials $u \in F_p[x]$.*

Corollary 2.30. *Let f be an irreducible polynomial of degree n in $F_p[x]$. If $d|(p^n - 1)$ then the congruence $u^d \equiv 1 \pmod{f}$ has exactly d solutions.*

Definition 2.6. *Let f and a be any two polynomials in $F_p[x]$, and suppose that $(a, f) = 1$. Let h be the least positive integer such that $a^h \equiv 1 \pmod{f}$. We say that the order of a modulo f is h, or that a belongs to the exponent h modulo f.*

Lemma 2.31. *Let a and f be polynomials in $F_p[x]$. If a has order h modulo f then $a^k \equiv 1 \pmod{f}$ if and only if $h|k$.*

Corollary 2.32. *Let a and f be polynomials in $F_p[x]$. If $(a, f) = 1$ then the order of a modulo f divides $p^n - 1$, where $n = \deg f$.*

Lemma 2.33. *Let a and f be polynomials in $F_p[x]$. If a has order h modulo f then a^k has order $h/(h, k)$ modulo f.*

Lemma 2.34. *Let a, b and f be polynomials in $F_p[x]$. If a has order h modulo f and b has order k modulo f, and $(h, k) = 1$, then ab has order hk modulo f.*

Definition 2.7. *Let f be a polynomial in $F_p[x]$. If g belongs to the exponent $\phi(f)$ then g is a* primitive root *modulo f.*

Lemma 2.35. *Let f be an irreducible polynomial of degree n in $F_p[x]$. If q is prime and $q^\alpha|(p^n - 1)$ where $\alpha \geq 1$, then there are precisely $q^\alpha - q^{\alpha-1}$ residue classes modulo f of order q^α.*

Theorem 2.36. *If f is an irreducible polynomial of degree n in $F_p[x]$ then there exist exactly $\phi(p^n-1)$ primitive roots modulo f.*

Theorem 2.37. *Let f be an irreducible polynomial of degree n in $F_p[x]$. If $(a,f)=1$ then the congruence $u^k \equiv a \pmod{f}$ has (k,p^n-1) solutions or no solution, according as*

$$a^{(p^n-1)/(k,p^n-1)} \equiv 1 \pmod{f},$$

or not.

The correspondence with numbering in NZM ends at this point.

Example 1. Let $p=2$. Then we have the polynomials $0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1,\ldots$. If a quadratic polynomial is reducible then it is the product of two linear polynomials. We note that $x^2=x^2$, $x(x+1)=x^2+x$, and that $(x+1)^2=x^2+1$. Thus three of the four quadratic polynomials available is reducible, but $f(x)=x^2+x+1$ is irreducible. A complete system of residues modulo f is given by $r_0=0$, $r_1=1$, $r_2=x$, $r_3=x+1$. By direct calculation we find that

$+$	r_0	r_1	r_2	r_3
r_0	r_0	r_1	r_2	r_3
r_1	r_1	r_0	r_3	r_2
r_2	r_2	r_3	r_0	r_1
r_3	r_3	r_2	r_1	r_0

$\times$	r_0	r_1	r_2	r_3
r_0	r_0	r_0	r_0	r_0
r_1	r_0	r_1	r_2	r_3
r_2	r_0	r_2	r_3	r_1
r_3	r_0	r_3	r_1	r_2

Here we see that r_2 and r_3 have order 3 $\pmod{f}$, so they are the primitive roots in this case.

Suppose that f is an irreducible polynomial of degree n in $F_p[x]$. We have shown that polynomials modulo f form a field, and that the multiplicative group of non-zero elements is cyclic. It is also easy to see that the additive group is isomorphic to $(C_p)^n$. More generally, if F is a finite field then by the pigeon-hole principle there is a positive integer n such that n=0. The least such positive integer is called the *characteristic* of the field. It is easy to see that if the characteristic of a field is finite, then it must be a prime number. The fields constructed above have p^n elements and characteristic p. It can also be shown that the number of elements in a finite field of characteristic p must be p^n for some n. The proof we have given that the multiplicative group of non-zero elements is cyclic generalizes to arbitrary finite fields. In §4 below we show that for every prime number p and every positive integer n there is at least one irreducible polynomial of degree n in $F_p[x]$. Hence there is a field of p^n elements. Finally, it can be shown that any two finite fields of the same size are isomorphic. Hence there is essentially only one field of size p^n. Note, however, that when n>1 the field of p^n elements is not the same as the ring of integers modulo p^n, which is not a field.

3. Derivatives

Definition 3.1. *If $f(x) = \sum_{i=0}^{n} a_i x^i$ is a polynomial, then the* derivative *of $f(x)$ is the polynomial $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.*

It is easy to verify that $(f(x) + g(x))' = f'(x) + g'(x)$, that $(cf(x))' = cf'(x)$, that $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$, and hence that $(f(x)^k)' = kf(x)^{k-1}f'(x)$. Suppose now that a and f are polynomials in $F_p[x]$, that f is irreducible, and that f divides a exactly to the power $\alpha > 0$, say $a = f^\alpha g$. Then $a' = \alpha f^{\alpha-1} f' + f^\alpha g'$, so that f divides a' to at least the power $\alpha - 1$. (If $p \nmid \alpha$ then the power is exactly $\alpha - 1$, but if $p|\alpha$ then the power is at least α.) Hence $(a, a') = 1$ if and only if a is square-free.

4. Further factorizations

Theorem 4.1. *If d and n are positive integers and $d|n$ then there is a polynomial $u(x)$ with integral coefficients such that $(x^d - 1)u(x) = x^n - 1$.*

Proof. Put $u(x) = x^{n-d} + x^{n-2d} + \cdots + x^d + 1$.

Corollary 4.2. *If a is an integer and d and n are positive integers such that $d|n$, then $(a^d - 1)|(a^n - 1)$.*

Theorem 4.3. *Let m and n be positive integers, and suppose that $(m, n) = g$. Then there exist polynomials $u(x)$ and $v(x)$ with integral coefficients such that*

$$(x^m - 1)u(x) + (x^n - 1)v(x) = x^g - 1.$$

Proof. Suppose that $m \ge n$, and write $m = q_1 n + r_1$ where $0 \le r_1 < n$. Then

$$x^{r_1} - 1 = (x^m - 1) - (x^{q_1 n} - 1)x^{r_1} = (x^m - 1)u_1(x) + (x^n - 1)v_1(x),$$

say. Next write $n = q_2 r_1 + r_2$ where $0 \le r_2 < r_1$, so that

$$x^{r_2} - 1 = (x^n - 1) - (x^{q_2 r_1} - 1)x^{r_2} = (x^m - 1)u_2(x) + (x^n - 1)v_2(x).$$

By continuing with the Euclidean algorithm, we eventually reach the last non-zero remainder r_j, and

$$x^{r_j} - 1 = (x^m - 1)u_j(x) + (x^n - 1)v_j(x).$$

Since $r_j = g$, this gives the result.

The calculation just completed is unusual in that each remainder polynomial is monic, so that when it is used as a divisor, the resulting quotient still has integral coefficients. Normally, if $p(x)$ and $q(x)$ are relatively prime polynomials with integral coefficients and one writes $p(x)u(x)+q(x)v(x)=1$, the coefficients of $u(x)$ and $v(x)$ are rational numbers. One can multiply by the least common denominator of these coefficients to obtain an identity of the form $p(x)u(x)+q(x)v(x)=c$; the least integer c that can be so expressed is of considerable significance and is called the *resultant* of the polynomials. Hence from the above we see that if $(m,n)=1$ then the resultant of x^m-1 and x^n-1 is 1.

Corollary 4.4. *Let m and n be positive integers, and put $g = (m, n)$. Then for any integer a, $(a^m - 1, a^n - 1) = a^g - 1$.*

Proof. Let $G = (a^m - 1, a^n - 1)$. Since $u(a)$ and $v(a)$ are integers it follows from Theorem 4.3 that $G|(a^g - 1)$. On the other hand, by Corollary 4.2 we see that $a^g - 1$ divides both $a^m - 1$ and $a^n - 1$. Hence $(a^g - 1)|G$, so that $G = a^g - 1$.

Theorem 4.5. *Let f be a polynomial in $F_p[x]$. Then $f(x)^p = f(x^p)$.*

Proof. Let u and v be any two polynomials in $F_p[x]$. Then $(u+v)^p = u^p + v^p$ since $p|\binom{p}{k}$ for $0 < k < p$. Hence by induction, $(u_1 + u_2 + \cdots + u_n)^p = u_1^p + u_2^p + \cdots + u_n^p$. Thus if $f(x) = \sum_i a_i x^i$ then $f(x)^p = \sum_i (a_i x^i)^p$. But $a_i^p \equiv a_i \pmod{p}$, so this is $\sum a_i x^{ip} = f(x^p)$.

Theorem 4.6. (Gauss) *Let $\mathcal{F}_n$ denote the set of all monic irreducible polynomials of degree n in $F_p[x]$. Then for any positive integer n,*

$$x^{p^n} - x = \prod_{d|n} \prod_{f \in \mathcal{F}_d} f(x). \tag{1}$$

The case $n = 1$ of this is already in §2.7 of NZM.

Proof. Let $h(x) = x^{p^n} - x \in F_p[x]$. Then $h'(x) = -1$. Hence $(h, h') = 1$, and so h is square-free. Thus to determine the factorization of g it is enough to determine which irreducible polynomials divide it.

Suppose that $d|n$, and that $f \in \mathcal{F}_d$. Then $(f, x) = 1$ unless $d = 1$ and $f(x) = x$, in which case $f|h$. Otherwise it follows by Theorem 2.8 that $x^{p^d - 1} \equiv 1 \pmod{f}$. That is, $f|(x^{p^d-1} - 1)$. But $(p^d - 1)|(p^n - 1)$ by Corollary 4.2, and hence $(x^{p^d-1} - 1)|(x^{p^n-1} - 1)$ by Theorem 4.1. Hence the right hand side displayed above divides the left hand side.

To complete the proof it suffices to show that if f is an irreducible monic polynomial of degree m that divides $x^{p^n} - x$ then $m|n$. If $f(x) = x$ then $m = 1$, and we are done, since $1|n$. Otherwise, $(f, x) = 1$, so from $f|(x^{p^n} - x)$ it follows by Theorem 1.10 that $f|(x^{p^n-1} - 1)$. We also know, by Theorem 2.7, that $f|(x^{p^m-1} - 1)$. Then by Theorem 4.3 it follows that $f|(x^{p^d-1} - 1)$, where $d = (m, n)$. That is, $x^{p^d-1} \equiv 1 \pmod{f}$, which implies that $x^{p^d} \equiv x \pmod{f}$. Let $g(x)$ be an arbitrary polynomial in $F_p[x]$. By d applications of Theorem 4.5 we see that $g(x)^{p^d} = g(x^{p^d})$. But this is $\equiv g(x) \pmod{f}$ by Theorem 2.2. Thus $g(x)^{p^d} \equiv g(x) \pmod{f}$. If $(g, f) = 1$ then we may cancel g from both sides, to see that $g(x)^{p^d-1} \equiv 1 \pmod{f}$. Now suppose that g is a primitive root of f. Then the order of g modulo f is $p^m - 1$, and so we deduce that $d \ge m$. But d is a divisor of m, so it follows that $d = m$. As d is also a divisor of n we conclude that $m|n$, and the proof is complete.

Corollary 4.7. *For each $n \ge 1$, there is at least on irreducible polynomial in $F_p[x]$ of degree n.*

Proof. By applying the identity $\deg ab = \deg a + \deg b$ in (1), we deduce that

$$p^n = \sum_{d|n} d \operatorname{card} \mathcal{F}_d. \tag{2}$$

By discarding the (non-negative) contribution of the terms for $d < n$, we deduce that

$$\text{card}\,\mathcal{F}_n \le \frac{p^n}{n} \tag{3}$$

for all n. By (2) we see that

$$n\ \text{card}\,\mathcal{F}_n = p^n - \sum_{\substack{d|n\\ d<n}} d\ \text{card}\,\mathcal{F}_d$$

which by (3) is

$$\begin{aligned}
&\ge p^n - \sum_{\substack{d|n\\ d<n}} p^d \\
&\ge p^n - \sum_{1\le d\le[n/2]} p^d \\
&\ge p^n - \frac{p^{[n/2]+1}-1}{p-1}.
\end{aligned}$$

Since $p \ge 2$, this is

$$\ge p^n - p^{[n/2]+1} + 1.$$

But $[n/2]+1 \le n$ for $n = 1, 2, 3, \ldots$, so the above is ≥ 1.

Corollary 4.8. *The number of monic irreducible polynomials of degree n in $F_p[x]$ is exactly*

$$\frac{1}{n}\sum_{d|n} \mu(d) p^{n/d}.$$

Proof. Apply the Möbius inversion formula to the identity (1).

It is somewhat curious that the sum above should always be divisible by n. Since p might lie in any reduced residue class modulo n, this suggests the first exercise below. In the second exercise we recover (2) without needing so much of the theory.

EXERCISES

1. Show (by an argument independent of the present context) that if $(a, n) = 1$, then

$$\sum_{d|n} \mu(d) a^{n/d} \equiv 0 \pmod{n}.$$

2. (a) Let n_k denote the total number of monic polynomials of degree k in $\mathbb{F}_p[x]$. Show that $n_k = p^k$.
(b) Let $P_1, P_2, \ldots$ be the irreducible monic polynomials in $\mathbb{F}_p[x]$, listed in some (arbitrary) order. Show that

$$\prod_{r=1}^{\infty} \left(1 + z^{\deg P_r} + z^{2\deg P_r} + z^{3\deg P_r} + \cdots\right) = 1 + pz + p^2z^2 + p^3z^3 + \cdots$$

for $|z| < 1/p$.
(c) Let g_k denote the number of irreducible monic polynomials of degree k in $\mathbb{F}_p[x]$. Show that

$$\prod_{k=1}^{\infty} \left(1 - z^k\right)^{-g_k} = (1 - pz)^{-1} \qquad (|z| < 1/p).$$

(d) Take logarithmic derivatives to show that

$$\sum_{k=1}^{\infty} k g_k \frac{z^{k-1}}{1 - z^k} = \frac{p}{1 - pz} \qquad (|z| < 1/p).$$

(e) Show that

$$\sum_{k=1}^{\infty} k g_k \sum_{m=1}^{\infty} z^{mk} = \sum_{n=1}^{\infty} p^n z^n \qquad (|z| < 1/p).$$

(f) Deduce that

$$\sum_{k|n} k g_k = p^n$$

for all positive integers n.
(g) (Gauss) Use the Möbius inversion formula to show that

$$g_n = \frac{1}{n} \sum_{k|n} \mu(k) p^{n/k}$$

for all positive integers n.
(h) Use (f) (not (g)) to show that

$$\frac{p^n}{n} - \frac{2p^{n/2}}{n} \leq g_n \leq \frac{p^n}{n}.$$

(i) If a monic polynomial of degree n is chosen at random from $\mathbb{F}_p[x]$, about how likely is it that it is irreducible? (Assume that p and/or n is large.)
(j) Show that $g_n > 0$ for all p and all $n \geq 1$. (If $P \in \mathbb{F}_p[x]$ is irreducible and has degree n, then the quotient ring $\mathbb{F}_p[x]/(P)$ is a field of p^n elements. Thus we have proved that there

is such a field, for each prime p and integer $n \geq 1$. It may be further shown that the order of a finite field is necessarily a primepower, and that any two finite fields of the same order are isomorphic. Hence the field of order p^n, whose existence we have proved, is essentially unique.)

3. (E. Berlekamp) Let p be a prime number. We recall that polynomials in a single variable (mod p) factor uniquely into irreducible polynomials. Thus a monic polynomial $f(x)$ can be expressed uniquely (mod p) in the form $g(x)h(x)^2$ where $g(x)$ is squarefree (mod p) and both g and h are monic. Let s_n denote the number of monic squarefree polynomials (mod p) of degree n. Show that

$$\left(\sum_{k=0}^{\infty} s_k z^k\right)\left(\sum_{m=0}^{\infty} p^m z^{2m}\right) = \sum_{n=0}^{\infty} p^n z^n$$

for $|z| < 1/p$. Deduce that

$$\sum_{k=0}^{\infty} s_k z^k = \frac{1 - pz^2}{1 - pz},$$

and hence that $s_0 = 1$, $s_1 = p$, and that $s_k = p^k(1 - 1/p)$ for all $k \geq 2$.