CHAPTER SIX

IRREDUCIBILITY AND FACTORIZATION

§1. BASIC DIVISIBILITY THEORY

The set of polynomials over a field **F** is a ring, whose structure shares with the ring of integers many characteristics. A polynomials is *irreducible* iff it cannot be factored as a product of polynomials of strictly lower degree. Otherwise, the polynomial is *reducible.* Every linear polynomial is irreducible, and, when $\mathbf{F} = \mathbf{C}$, these are the only ones. When $\mathbf{F} = \mathbf{R}$, then the only other irreducibles are quadratics with negative discriminants. However, when $\mathbf{F} = \mathbf{Q}$, there are irreducible polynomials of arbitrary degree.

As for the integers, we have a division algorithm, which in this case takes the form that, if $f(x)$ and $g(x)$ are two polynomials, then there is a quotient $q(x)$ and a remainder $r(x)$ whose degree is less than that of $g(x)$ for which

$$f(x) = q(x)g(x) + r(x) \ .$$

The *greatest common divisor* of two polynomials $f(x)$ and $g(x)$ is a polynomial of maximum degree that divides both $f(x)$ and $g(x)$. It is determined up to multiplication by a constant, and every common divisor divides the greatest common divisor. These correspond to similar results for the integers and can be established in the same way. One can determine a greatest common divisor by the Euclidean algorithm, and by going through the equations in the algorithm backward arrive at the result that there are polynomials $u(x)$ and $v(x)$ for which

$$\text{gcd } (f(x), g(x)) = u(x)f(x) + v(x)g(x) \ .$$

Two polynomials are *coprime* if their greatest common divisor is 1. If a polynomial $p(x)$ divides a product $f(x)g(x)$ and is coprime with one of the factors, then it must divide the other. Thus, an irreducible polynomial that divides a product of any number of polynomials must divide one of the factors. Each polynomial can be written as the product of irreducibles in a unique way up to order of factors and multiplication by constants.

Thus, it is desirable to have a way of determining when a polynomial is irreducible, and, more generally, how to factor it.

A result for integers that has an analogue for polynomials is the *Chinese Remainder Theorem*: *Suppose that $f_1, f_2, \cdots, f_k$ are pairwise coprime polynomials over a field* **F** *and $g_1, g_2, \cdots, g_k$ are arbitrary polynomials. Then there exists a polynomial $h(x)$ for which $h \equiv g_i$ (mod f_i) which is uniquely determined up to a multiple of $f_1 f_2 \cdots f_k$.*

§2. IRREDUCIBLE POLYNOMIALS

Newton's Polygon. Suppose that $f(t) = \sum A_i t^i$ is a polynomial with integer coefficients, and that p is a positive prime integer. If we write $A_i = a_i p^{\alpha_i}$, where a_i is not divisible by p, then we can define the *Newton polygon* for f with respect to p as follows: For each i, plot the point (i, α_i) in the cartesian plane. The Newton polygon is an open polygon which forms the lower boundary of the convex hull of these points, so that all of these points lie either on or above the polygon. This polygon consists of a finite number of line segments, whose slopes can be listed in increasing order. It may happen that two segments in the Newton polygon are collinear, in which case a slope may be listed more than once. The *Dumas' theorem* states that, *if $f = gh$ is a factorization of a polynomial as a product of polynomials of lower degree over* **Z**, *then the set of slopes for the Newton polygon of f is the union of the sets of slopes for the Newton polygons of g and h.* Moreover, if we weight each slope according to the differences of the abscissae of the endpoints of the segment, then the sum of the weights for g and h is equal to the weight for f. Since a proof of this appears in [**3**], I will illustrate the theorem with an example.

Let

$$g(t) = p^4 + p^2t + t^2 + pt^3 + p^3t^4 + p^3t^5 \ .$$

The points plotted in the cartesian plane (with those actually on and defining the Newton polygon in boldface) are:

$$(\mathbf{0},\mathbf{4}),(\mathbf{1},\mathbf{2}),(\mathbf{2},\mathbf{0}),(\mathbf{3},\mathbf{1}),(4,3),(\mathbf{5},\mathbf{3})$$

with the list of slopes $\{-2,-2,1,1\}$. Let

$$h(t) = p + p^2t + p^2t^2 + pt^3 + p^4t^4 \ .$$

The set of points (with those on the Newton polygon in boldface) are:

$$(\mathbf{0},\mathbf{1}),(1,2),(2,2),(\mathbf{3},\mathbf{1}),(\mathbf{4},\mathbf{4})$$

with the list of slopes $\{0,3\}$.

The product $f(x) = g(x)h(x)$ of these polynomials is

$$\begin{aligned} f(x) = p^5 + p^3(1+p^3)t + p(1+p^3+p^5)t^2 + p^2(2+p^2+p^3)t^3 + p^2(1+2p+p^2+p^6)t^4 \\ + p(1+p^2+p^3+p^4+p^5)t^5 + p^2(1+p^2+2p^3)t^6 + p^4(1+2p)t^7 + p^4(1+p^3)t^8 + p^7t^9 \ . \end{aligned}$$

The corresponding set of points is

$$(\mathbf{0},\mathbf{5}),(\mathbf{1},\mathbf{3}),(\mathbf{2},\mathbf{1}),(3,2),(4,2),(\mathbf{5},\mathbf{1}),(\mathbf{6},\mathbf{2}),(7,4),(\mathbf{8},\mathbf{4}),(\mathbf{9},\mathbf{7})$$

with slope list $\{-2,-2,0,1,1,3\}$.

Each of these points, considered as a $2-$vector, is the sum of $2-$vectors for g and h corresponding to the terms in g and h whose product gives the smallest power of p in the coefficient of the power of t that corresponds to the point. Thus:

$$(0,5) = (0,4) + (0,1); (1,3) = (1,2) + (0,1); (2,1) = (2,0) + (0,1);$$

$$(3,2) = (2,0) + (1,2) = (3,1) + (0,1); (4,2) = (2,0) + (2,2); (5,1) = (2,0) + (3,1);$$

$$(6,2) = (3,1) + (3,1); (7,4) = (4,3) + (3,1); (8,4) = (5,3) + (3,1); (9,7) = (5,3) + (4,4).$$

Each vertex of the Newton polygon of f is a vector sum of vertices of the Newton polygon of g and h.

To understand why the Dumas result holds, consider a particular slope, 1, that is listed twice for the product f. This arises from the pair of edges of the Newton polygon containing the three collinear points $(5,1),(6,2),(8,4)$. These lie on the line $y-x=-4$. The number -4 is the smallest value of $y-x$ assumed at any of the points on or above the polygon. Let us call these values of $y-x$ the *weight* of $y-x$ at the points in question.

The weight of $(5,1)$, $(6,2)$, $(8,4)$ are each equal to the sum of the weights of the vertices of the Newton polygon of g and h whose vector sum they are. In this case, $(3,1)$ figures in each sum, so the weight of the summands $(2,0)$, $(3,1)$ and $(5,3)$ must be the same. There cannot be vertices of lesser weight than these three for g, nor vertices of lesser weight than $(3,1)$ for h, because these would combine to give a point of lesser weight corresponding to a term in the product f.

Thus, for the points corresponding to $g(t)$, this function $y-x$ is minimized among the points for h at $(3,1)$, and, among the points for g, at $(2,0),(3,1),(5,3)$. Therefore, the line $y-x=-2$ contains two collinear edges of the Newton polygon and its slope 1 gets listed twice for g.

To illustrate how a slope for a factor can appear among the slopes for the product, consider the slope 3 in the list for h. This corresponds to the edge joining $(3,1)$ and $(4,4)$, at each of which the function $y-3x$

has weight -8. Among the vertices for g, the weight of $y - 3x$ is minimized at $(5, 3)$, and two vertices of the Newton polygon for f involving these points are

$$(8,4) = (3,1) + (5,3) \quad \text{and} \quad (9,7) = (4,4) + (5,3) \ .$$

The weight of $y - 3x$ at each of these points is minimized and we have one edge of the Newton polygon of slope 3.

This analysis can be adapted to the situation for which a slope is listed more than once for each of the factors in the product. In this case, the corresponding weight function is minimized at more than one vertex of the Newton polygon for each of the factors, and the vertices for one of the factors can be combined with the vertex of minimum weight for the other to give a minimizing set of vertices with the same cardinality for the product.

As a corollary, if, for some prime, the Newton polygon consists of precisely one segment, then it must be irreducible. In particular, we have the *Eisenstein irreducibility criterion*: *If $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is a polynomial over $\mathbf{Z}$ and p is a prime that does not divide a_n, but divides all the other coefficients, and p^2 does not divide a_0, then $f(x)$ is irreducible over $\mathbf{Z}$.*

An example of an irreducibility result of a different character is *Perron's criterion*: *Suppose that $u(x) = x^n + \cdots + a_1 x + a_0$ is a polynomial over $\mathbf{Z}$ for which $a_0 \neq 0$ and*

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0| \ .$$

Then f is irreducible.

We use Rouché's theorem to show that $u(z)$ has precisely one zero in the exterior of the open unit disc D. This is true of the polynomial $v(z) = z^n + a_{n-1} z^{n-1}$ since $|a_{n-1}| > 1$. Observe that, when $|z| = 1$,

$$|u(z) - v(z)| \leq |a_{n-2}| + \cdots + |a_0| < |a_{n-1}| - 1 \leq |v(z)| \ .$$

Suppose, if possible, that u can be written as the product of two monic polynomials u_1 and u_2, both of which must have nonzero constant coefficient. The the product of the zeros for each of u_1 and u_2 must be an integer, and so each must have a zero that lies outside of D; but then u would have two such zeros, contradicting what was established.

Finally, we have *Hilbert's Irreducibility Theorem*: *If $f(t, x)$ is an ireducible polynomial over $\mathbf{Q}$, then there are infinitely many rational values of t for which the polynomial $f_t(x) \equiv f(t, x)$ is irreducible over $\mathbf{Q}$.*

§3. PRIMES AND REDUCIBLE POLYNOMIALS

Is there a connection between polynomials that are irreducible over $\mathbf{Z}$ and polynomials that assume prime values for integer values of its argument? Of course, the values of a polynomial can never be prime, even when it is irreducible, when there is a nontrivial common divisor of its coefficients. So we restrict attention to polynomials over $\mathbf{Z}$ that are *primitive*, that is, for which the greatest common divisor of the coefficients is 1.

Dirichlet showed that, in every positive arithmetic progression whose initial term and common difference are coprime, there are infinitely many primes. In other words, every linear polynomial $dx + b$, with b and d coprime, is prime for infinitely many integers x. For polynomials of higher degree, the corresponding situation is unknown. For example, it still needs to be settled whether there are infinitely many primes of the form $x^2 + 1$ for integer x.

In the other direction, suppose that a polynomial $f(x)$ can be factored as a product of two nonconstant polynomials $f(x) = g(x)h(x)$ over $\mathbf{Z}$. Every time that $|f(x)|$ assumes a prime value for integral x, one of the factors $g(x)$ and $h(x)$ must take one of the values 1 and -1. Since any polynomial can assume a value finitely often, the absolute value of $f(x)$ is prime for only finitely many integers. Thus, if the absolute value of a polynomial assumes sufficiently many prime values (trivially, more than four times the degree of $f(x)$), it must be irreducible.

In fact, under some circumstances, it is enough that a polynomial assumes a prime value once in order to be irreducible. A theorem of A. Cohn is that, if $p = \sum_{k=0}^{n} a_k 10^k$ is the base 10 representation of a prime p (with $0 \leq a_k \leq 9$), then $f(x) = \sum_{k=0}^{n} a_k x^k$ is irreducible over $\mathbf{Z}$. In fact, we have the corresponding result when 10 is replaced by any integer base b exceeding 1. However, the positivity of the a_k plays a role; as the examples $x^3 - 9x^2 - 9x + 1 = (x+1)(x^2 - 10x + 1)$ and $x^3 - 9x^2 + x - 9 = (x-9)(x^2+1)$ demonstrate, it is possible for the value when $x = 10$ to be prime even though the polynomial is reducible.

A result similar to Cohn's theorem was established by Murty [**2**]. Murty made a small technical adaptation to his result to obtain Cohn's theorem. However, the approach is illustrated by the following generalization of Murty's result by Girstmair [**1**]:

Let $f(x) = \sum_{k=0}^{n} a_k x^k$ be a primitive polynomial of positive degree n. Suppose that H is the maximum of $|a_k/a_n|$ for $0 \leq k \leq n$, and that d and n are positive integers for which $n \geq H + d + 1$ and $|f(n)| = dp$ for some prime number p not dividing d. Then $f(x)$ is irreducible over $\mathbf{Z}$.

The proof begins with the observation that each zero r of $f(x)$ satisfies $|r| < H + 1$ (see Section 1.2). Suppose if possible that $f(x) = g(x)h(x)$ for two polynomials $g(x)$ and $h(x)$ over $\mathbf{Z}$ of positive degree. Then $g(x) = c\prod(x - r)$ where c is the leading coefficient of $g(x)$ and the product is over a nonvoid subset of the zeros of $f(x)$.

Since $|f(n)| = |g(n)h(n)| = dp$ and p does not divide d, one of the factors, say $g(n)$ is coprime with p and so must divide d. But then, for each zero r of $f(x)$,

$$|n - r| \geq n - |r| > (H + d + 1) - (H + 1) = d \ ,$$

so that $|g(n)| > d$. This yields a contradiction and we can deduce that the factorization of $f(x)$ is not possible. ♠.

Let us return to the question of how often the absolute value of a reducible polynomial over $\mathbf{Z}$ can be prime. Consider first the case that $f(x)$ is quadratic. If it is reducible, it is the product of two linear polynomials. Since each linear polynomial can assume each of the values 1 and -1 at most once, we see that a reducible quadratic can be prime at most four times. This is possible, the absolute value of the quadratic

$$f(x) = -4x^2 + 12x - 5 = 4 - (2x - 3)^2 = (5 - 2x)(2x - 1)$$

is prime when $x = 0, 1, 2, 3$.

A reducible cubic must be factorable as a product of a linear and a quadratic polynomial. The quadratic polynomial $s(x) = x^2 + x - 1$ takes the value $+1$ when $x = -2, 1$, and the value -1 when $x = -1, 0$, so it takes the values ± 1 four times, which is the maximum possible for a quadratic. These can possibly be matched against prime values of the linear cofactor. The linear cofactor can also takes each of the values 1 and -1 at most once, and it might be possible to match these with prime values of the quadratic. However, a quadratic assuming the value ± 1 four times is essentially $s(x)$ up to horizontal translation and multiplication by -1 and a linear polynomial assuming both values ± 1 must assume them for arguments that differ by at most 2. So in fact, it can be seen that the absolute value of a reducible cubic can be prime at most five times. The example

$$f(x) = -6x^3 + 5x^2 + 17x - 11 = (x^2 + x - 1)(11 - 6x)$$

delivers this, as it takes the values 23, -17, -11, 5 and -5 when $x = -2, -1, 0, 1, 2$.

A reducible quartic must be factorable either as a product of a cubic and a linear polynomial or as the product of two quadratics. The cubic can take the values 1 and -1 each at most three times, so it can be seen that the absolute value of the quartic can be prime at most eight times (the linear factor providing the prime six times and the cubic factor twice). Each of the quadratic factors can take the values 1 and -1 at most twice, so again the absolute value of the quartic can be prime at most eight times. This is achievable with the quartic

$$f(x) = x^4 + 2x^3 - 9x^2 - 10x + 5 = (x^2 + 5x + 5)(x^2 - 3x + 1) = s(x + 2)s(x - 2)$$

whose absolute value is prime for integers x satisfying $-4 \leq x \leq 3$.

§4. FACTORIZATION OF POLYNOMIALS OVER THE INTEGERS

One simple way to get at a factor of a polynomial $f(x)$ is to determine the greatest common divisor of it and its derivative. If this common divisor is 1, then every irreducible factor of $f(x)$ appears only to the first degree. If this common divisor has positive degree, then we have a divisor of the polynomial. The quotient with respect to this divisor will be a product of irreducibles, all raised to the exponent 1.

There is a test to show whether two polynomials have a divisor in common. Suppose that $f(x)$ is a polynomial of degree n and that $g(x)$ is a polynomial of degree m. Then f and g have a nontrivial common divisor h if and only if there are polynomials p and q of degrees not exceeding $n - 1$ and $m - 1$ respectively, for which $f = hp$ and $g = hq$. If this happens, then $fq = gp$.

On the other hand, suppose that $fq = gp$ for some polynomials p and q for which the degrees of p and q do not exceed $n - 1$ and $m - 1$ respectively. Then f and g cannot be coprime. For otherwise, f, dividing the product gp, would have to divide p, which is impossible.

Finding such a pair p, q of polynomials entails setting up a set of linear equations for its coefficients in terms of the coefficients of f and g. To see how this works, suppose, for example, that

$$f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \ ,$$

$$g(x) = b_2x^2 + b_1x_1 + b_0 \ ,$$

$$p(x) = u_2x^2 + u_1x + u_0 \ ,$$

$$q(x) = v_1x + v_0 \ .$$

Comparing the coefficients on either side of the equation $f(x)q(x) = g(x)p(x)$ leads to the linear system

$$a_3v_1 = b_2u_2$$

$$a_2v_1 + a_3v_0 = b_1u_2 + b_2u_1$$

$$a_1v_1 + a_2v_0 = b_0u_2 + b_1u_1 + b_0u_0$$

$$a_1v_0 + a_0v_1 = b_0u_1 + b_1u_0$$

$$a_0v_0 = b_0u_0 \ ,$$

whose associated matrix of coefficients is

$$\begin{pmatrix} a_3 & 0 & -b_2 & 0 & 0 \\ a_2 & a_3 & -b_1 & -b_2 & 0 \\ a_1 & a_2 & -b_0 & -b_1 & -b_2 \\ a_0 & a_1 & 0 & -b_0 & -b_1 \\ 0 & a_0 & 0 & 0 & -b_0 \end{pmatrix}$$

A pair (p, q) of polynomials exists if and only if the determinant of the matrix, or equivalently of the matrix

$$\begin{pmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{pmatrix}$$

vanishes. This determinant is called the *Sylvester resultant* of the polynomials f and g.

If a polynomial over $\mathbf{Z}$ is reducible, then if we reduce its coefficients modulo a prime p, with a finitely many exceptions where the prime figures in the factors of the coefficients, it will still factor. Accordingly, the task of factoring a polynomial can be carried out modulo p for primes p, and then the architecture of the factorizations examined to suggest possible factorizations over the integers.

A standard algorithm for the modulo p factorization is due to Berlekamp. We have the following results for a monic polynomial $f(x)$ of degree n.

Suppose h is such that $h^p - h$ is divisible by f modulo p; then

$$f(x) = \prod_a \{ \text{ gcd } (f(x), h(x) - a) : a \in \mathbf{Z}_p \} \ .$$

To prove this, we note that, modulo p, the polynomials $h(x) - a$ constitute a coprime set as a varies over $\mathbf{Z}_p$, so that the polynomial

$$F(x) = \prod_a \text{ gcd } (f(x), h(x) - a)$$

is a product of pairwise coprime polynomials and so a divisor of $f(x)$. However, it is given that $f(x)$ divides

$$h(x)^p - h(x) = \prod_a (h(x) - a) \ .$$

Suppose that $h(x) - a = u_a(x)v_a(x)$, where $u_a(x)$ is the greatest common divisor of $f(x)$ and $h(x) - a$, and $f(x)$ and $v_a(x)$ are coprime. Then $f(x)$ divides

$$\prod_a u_a(x) \prod_a v_a(x) \ .$$

Since the second product is coprime with $f(x)$ and the first product is equal to $F(x)$, it follows that $f(x)$ divides $F(x)$. Hence, $f(x) = F(x)$. □

To effect this algorithm, we need to construct a function h for which $h^p - h$ is divisible by f. How this is done will be illustrated by an example. Suppose we wish to factor over the integers the polynomial

$$f(x) = x^5 + x^4 + 3x^3 + x^2 - 2x + 8 \ .$$

Let a test prime p be 3, and suppose that $h(x) = ax^4 + bx^3 + cx^2 + dx$, where a, b, c, d are to be determined. Since we wish to examine $h(x) - a$ for values of a modulo 3, we can assume that the constant term of $h(x)$ is 0. When we evaluate $h(x)^p$, for any prime p, the coefficients of all the terms except for the pth power of ax^4, bx^3, cx^2, dx are divisible by p. Also, by Fermat's Little Theorem, $k^p \equiv k \pmod p$ for each integer k. Therefore, modulo 3,

$$h(x)^3 \equiv ax^{12} + bx^9 + cx^6 + dx^3 = h(x^3) \ .$$

Since we want to select the coefficients so that $h^p - h$ is divisible by f, we determine $h(x^3)$ modulo $f(x)$.

We can determine the polynomial of degree less than 5 congruent to x^6, x^9, x^{12} modulo f, for example, by taking the remainder when the monomial is divided by f. Thus,

$$x^6 \equiv x^4 + 2x^3 + 2x + 2 \ ;$$

$$x^9 \equiv 2x^4 + x^2 + 2x + 2 \ ;$$

$$x^{12} \equiv 2x^3 + x^2 + x \ .$$

Therefore

$$ax^{12} + bx^9 + cx^6 + dx^3 \equiv (2b+c)x^4 + (2a+2c+d)x^3 + (a+b)x^2 + (a+2b+2c)x + 2(b+c) \ .$$

Equating $h(x)$ and $h(x^3)$ (mod $f(x)$), leads to the equivalences, modulo 3,

$$2b + c \equiv a \ , \quad 2a + 2c + d \equiv b \ , \quad a + b \equiv c \ , \quad a + 2b + 2c \equiv d \ , \quad b + c \equiv 0 \ .$$

These are satisfied by $(a, b, c, d) \equiv (1, 1, 2, 1)$ (mod 3). Thus, $h(x) = x^4 + x^3 + 2x^2 + x$.

We find that gcd $(h(x), f(x)) = 1$, gcd $(h(x)+1, f(x)) = x^2+x+1$, and gcd $(h(x)+2, f(x)) = x^3+2x+2$. Indeed, modulo 3,

$$h(x) + 1 \equiv x^4 + x^3 + 2x^2 + x + 1 \equiv (x^2 + x + 1)(x^2 + 1) \ ;$$

$$h(x) + 2 \equiv x^4 + x^3 + 2x^2 + x + 2 \equiv (x^3 + 2x + 2)(x + 1) \ ;$$

and

$$f(x) \equiv x^5 + x^4 + x^2 + x + 2 \equiv (x^2 + x + 1)(x^3 + 2x + 2) \ .$$

This indicates that we should find a factorization of $f(x)$ as a product of a quadratic and a cubic, where the coefficients, modulo 3, are given as above. Since the constant coefficient of $f(x)$ is equal to 8, this suggest that we try 4 as the constant of the quadratic factor and 2 as the constant of the cubic. A little trial and error leads to

$$f(x) = (x^2 + x + 4)(x^3 - x + 2) \ .$$

In practice, we can try the factorization with different primes, and then "lift" these to surmise the desired coefficients of the factors.

§5. PROBLEMS AND INVESTIGATIONS

1. Let $a_1, a_2, \cdots, a_n$ be distinct integers. Prove that the polynomial $(x - a_1)^2(x - a_2)^2 \cdots (x - a_n)^2 + 1$ cannot be factored as the product of two nonconstant polynomials with integer coefficients.

2. Let $P_n(x) = (x + 1)^n - x^n - 1$. Prove that $P_n(x)$ can be factored as a product

$$x(x + 1)^a(x^2 + x + 1)^b Q_n(x)$$

where $a = b = 0$ when n is even, $a = 1$ when n is odd, and $b = 0, 1, 2$ according as $n \equiv 3, 5, 1$ (mod 6). Investigate the factorization of $Q_n(x)$. D. Miramanoff conjectured that $Q_n(x)$ is irreducible whenever n is prime.

3. Suppose that p is a prime. Prove that $z^4 + 1$ can be written as the product of two quadratic factors modulo p. Are these factors irreducible?

4. Find all monic polynomials p such that $p(n)$ divides $p(n^2)$ for every positive integer n.

5. Let n be a positive integer, and Φ_n be the polynomial of minimum degree over $\mathbf{Q}$ whose root is a priomitive nth root of unity (the nth cyclotomic polynomial, whose degree is $\phi(n)$, where ϕ is Euler's totient

function). For pairs (m, n) of unequal positive integers, determine the smallest natural number k for which there are integers a and b for which $a\Phi_m + b\Phi_n = k$.

6. Give examples of polynomials $p(x)$ of small degree over $\mathbf{Z}$ whose absolute values are prime as often as possible for integer values of x.

7. (a) Is there a quadratic polynomial f with rational coefficients for which the quartic f^2+1 is reducible over the rationals?

(b) Is there a quadratic polynomial g with rational coefficients for which the octic $g^4 + 1$ is reducible over the rational?

Hints and comments.

2. See the paper D. Miramanoff, Sur l'équation $(x + 1)^l - x^l - 1 = 0$. *Nouv. Ann. Math.* 3 (1903), 385-397.

3. When p is a prime congruent to 1 modulo 4, then -1 is a square modulo p; when p is a prime congruent to 3 modulo 4, then either 2 or -2 is a square modulo p.

4. [AMM #10802: 107 (2000), 462; 109:6 (June-July, 2002), 570]

5. [AMM #10914: 109:1 (January, 2002), 77; 110:8 (October, 2003(, 745]

6. For example, the functions $| - 4x^2 + 2x - 5| = |(5 - 2x)(2x - 1)|$, $| - 6x^3 + 5x^2 + 17x - 11| = |(x^2 + x - 1)(11 - 6x)|$, $|x^4 + 2x^3 - 9x^2 - 10x + 5| = |(x^2 + 5x + 5)(x^2 - 3x + 1)|$ are prime, respectively, when the integer x satisfies $0 \le x \le 3$, $-2 \le x \le 2$, $-7 \le x \le 5$.

7. (a) $(x^2 - \frac{3}{4})^2 + 1 = x^4 - \frac{3}{2}x + \frac{25}{16} = (x^2 - 2x + \frac{5}{4})(x^2 + 2x + \frac{5}{4})$.

(b) [AMM # : 114:3 (March, 2007), 260]

References

1. K. Girstmair, On an irreducibility criterion of M. Ram Murty. *American Math. Monthly* 112:3 (March, 2005), 269-270
2. D. Miramanoff, *Sur l'équation* $(x + 1)^l - x^l - 1 = 0$. *Nouvelle Annales de Math'ematiques* 4 série, 3 (1903), 385-397
3. M. Ram Murty, Prime numbers and irreducible polynomials. *American Math. Monthly* 109:5 (May, 2002), 452-458
4. Victor V. Prasolov, *Polynomials.* Springer
   Chapter 2 (pages 47-76)