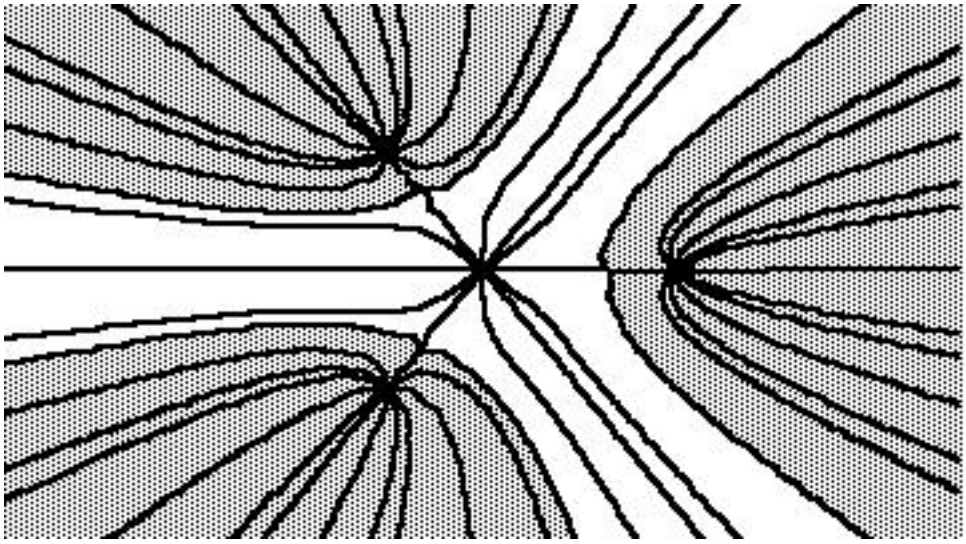
Theory of Equations

Lesson 11

by

Barry H. Dayton
Northeastern Illinois University
Chicago, IL 60625, USA

www.neiu.edu/~bhdayton/theq/



Chapter 5

Number Theory

FACTORING INTEGER POLYNOMIALS

In this chapter we discuss the special properties of polynomials with integer or rational coefficients with special attention given to factoring. Not only has this been studied extensively over the last 400 years, but the theory is useful in many modern applications such as coding theory.

5.1 Rational Polynomials and Algebraic Numbers

The set of rational numbers, which we denote by $\boldsymbol{Q}$, is the set of all fractions $\frac{m}{n}$ where m, n are integers with $n > 0$. $\boldsymbol{Q}$ satisfies all the field axioms C1,C2, R1 - R8 and F1 of §1.1 and so we call the set of rational numbers a *field*. The rational numbers also satisfy O1, O2, and O3 but not O4, but this will not be of much interest to us.

The set of polynomials with rational coefficients will be denoted $\boldsymbol{Q}[x]$ and satisfies many algebraic properties similar to the real or complex polynomials. All the results of §1.4, 1.5, 1.6 and 1.8 hold for $\boldsymbol{Q}[x]$, as do most of the results of §1.7, especially Theorems 1.5.1, 1.6.1, 1.6.2, 1.7.1, 1.7.2, 1.7.3, 1.8.2 and the Euclidean Algorithm which all simply depend on the set of coefficients being a field. When we speak of factoring a polynomial in $\boldsymbol{Q}[x]$ we mean for the factors also to be rational polynomials in $\boldsymbol{Q}[x]$, thus $p(x)|f(x)$ as polynomials in $\boldsymbol{Q}[x]$ means that $f(x) = p(x) * q(x)$ where also $q(x) \in \boldsymbol{Q}[x]$. Note that Theorem 1.7.1 applied to $\boldsymbol{Q}[x]$ then says that $(x - c)$ is a factor of $p(x)$ if and only if c is a *rational* root of $p(x)$. Likewise the definitions of *irreducible* and *prime* refer to factoring in $\boldsymbol{Q}[x]$. Even with these restrictions, Theorems

1.9.3 and 1.9.4 still hold for $\boldsymbol{Q}[x]$, the proofs being exactly the same as in the real or complex case. There are, however, no analogs of the remaining theorems of §1.9 and there are irreducible polynomials of all degrees in $\boldsymbol{Q}[x]$. We will more fully discuss factorization in $\boldsymbol{Q}[x]$ in the next sections.

A complex number c is called *algebraic* if c is a root of a polynomial with rational coefficients. Thus $c = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ is an algebraic number because it is a solution of $x^3 - 1 = 0$. Not all real or complex numbers are algebraic. For example numbers such as e and π are not. Numbers which are not algebraic are called *transcendental*. Hermite first showed the transcendence of e in 1844 (an elementary, although long, proof of the transcendence of e is given in the text by I.Herstein, *Topics in Algebra*) and Lindemann showed the transcendence of π in 1882. One of Hilbert's famous problems was to decide which complex numbers are algebraic.

As there are uncountably many real and complex numbers the following result, which follows from set theory and the fact that a given rational polynomial can have only finitely many complex roots, says that "most" real or complex numbers are not algebraic:

Theorem 5.1.1 *The set of algebraic numbers is countable, i.e. can be put in a 1–1 correspondence with the positive integers.*

Given an algebraic number c, there is, by definition, at least one rational polynomial so that c is a root. A monic rational polynomial of smallest degree which has c as a root is called the *minimal polynomial* for c. For example if $c = -1/2 + i\sqrt{3}/2$, c is a root of $x^3 - 1$ but $x^2 + x + 1$ is the minimal polynomial for c.

Theorem 5.1.2 *Let c be an algebraic number with minimal polynomial $p(x)$. If $f(x) \in \boldsymbol{Q}[x]$ satisfies $f(c) = 0$ then $p(x)|f(x)$ in $\boldsymbol{Q}[x]$.*

Proof: By the division algorithm $f(x) = p(x) * q(x) + r(x)$ where $r(x)$ is 0 or of smaller degree than $p(x)$. If $r(x)$ is not 0 the fact that $r(c) = f(c) - p(c) * q(c) = 0$ contradicts $p(x)$ being the minimal polynomial.

There are a number of implications of Theorem 5.1.2. One is that the minimal polynomial is unique. A second is that the minimal polynomial is irreducible and conversely a monic irreducible polynomial $p(x)$ satisfying $p(c) = 0$ must be the minimal polynomial. Finally, Theorem 5.1.2 says that roots of rational polynomials come in clusters: if $f(x) \in \boldsymbol{Q}[x]$ and c is a root of $f(x)$ then z is also a root of $f(x)$ for every root z of the minimal polynomial $p(x)$ of c. A consequence of the fact that the minimal polynomial is irreducible is that by Theorem 1.11.3 all the roots of a minimal polynomial are distinct.

Maple Implementation

Minimal polynomials of decimal approximations of a real number can often be found by Maple. Essentially Maple finds an interpolating polynomial with integer coefficients satisfying the one condition that $p(c) = 0$ using the lattice algorithm as described in section 2.15. However, to make it easier they have a special routine which does the work of setting up the equations for you, especially in the case c is a complex number where real and imaginary parts need to be separated.

In older versions of maple the procedure is minpoly in the `polytools` package, use `with(polytools, minpoly);` to access this procedure. The command

```
minpoly(c,n);
```

gives the polynomial of degree n with "small" integer coefficients that comes closest to satisfying $p(c) = 0$. Try several degrees to find the correct polynomial. In later versions of Maple this is being replaced by the procedure `MinimalPolynomial` in the `PolynomialTools` package which does the same thing.

5.2 Integer Polynomials

In this chapter we are mainly interested in polynomials with integer coefficients. The set of all such polynomials is denoted by $\boldsymbol{Z}[x]$ where $\boldsymbol{Z}$ denotes the ring of integers $0, \pm 1, \pm 2, \ldots$. The ring $\boldsymbol{Z}$ itself is what we have called an *integral domain*, i.e. $\boldsymbol{Z}$ satisfies axioms C1, C2, R1-R8 and I1, but does not satisfy F1 of §1.1. Subsequently we do have polynomial addition and multiplication in $\boldsymbol{Z}[x]$ and Theorem 1.5.1 holds. Thus $\boldsymbol{Z}[x]$ also is an integral domain. But Theorem 1.6.1, the division algorithm, holds only in the following limited sense, since it is understood that in working with $\boldsymbol{Z}[x]$ we can do only integer arithmetic:

Theorem 5.2.1 *Given polynomials $f(x), g(x) \in \boldsymbol{Z}[x]$ with $g(x)$ a* **monic** *polynomial then there exist unique polynomials $q(x), r(x) \in \boldsymbol{Z}[x]$ so that $f(x) = g(x) * q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.*

Theorem 5.2.1 is strong enough to prove analogs of Theorems 1.7.1, 1.7.2 and 1.7.3 however Theorem 1.8.2, the greatest common divisor theorem, does not hold

in the given form. For example it can be seen that the polynomials $f(x) = x^3$ and $g(x) = x^2 - 3$ have greatest common divisor 1, but there is no way to write

$$1 = u(x) * f(x) + v(x) * g(x)$$

where $u(x), v(x) \in \boldsymbol{Z}[x]$. We will see that we have unique factorization and greatest common divisors, but we will have to take a roundabout route.

When factoring, a special concern with integer polynomials is that the coefficients themselves may need to be factored. The integers 1 and -1 are the only integers which have multiplicative inverses, we call them *units*. These units are ignored in factoring, other integer coefficients (or constant polynomials) do have to be considered. We will see that when working with integer polynomials, the concepts of *prime* and *irreducible* are different. We start out our consideration of factorization with the following idea.

Definition 5.2.2 Given an integer polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where each $a_j \in \boldsymbol{Z}$, the *content* c_f is the greatest common divisor of $\{a_0, a_1, \ldots, a_n\}$, i.e. $\pm$ the largest positive integer which divides all the a_j. If the content c_f is a unit, i.e. ± 1, we say $f(x)$ is *primitive*.

The next theorem says we can extend the notion of content to rational polynomials.

Theorem 5.2.3 *Any non-zero polynomial $f(x) \in \boldsymbol{Q}[x]$ can be factored in the form $f(x) = c_f f^*(x)$ where $c_f \in \boldsymbol{Q}$ and $f^*(x)$ is a primitive polynomial in $\boldsymbol{Z}[x]$. c_f, also called the* content of $f(x)$*, and $f^*(x)$ are unique up to sign.*

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$. The we can find a least common denominator d for the fractions a_j, i.e. $a_j = \frac{b_j}{d}$ where $\gcd\{b_0, \ldots, b_n, d\} = 1$. So take $c_f = \frac{e}{d}$ where $e = \gcd\{b_0, \ldots, b_n\}$ and $f^*(x) = \frac{b_0}{e} + \frac{b_1}{e}x + \cdots + \frac{b_n}{e}x^n$.

Theorem 5.2.4 (Gauss' Lemma) *The product of two primitive polynomials in $\boldsymbol{Z}[x]$ is primitive.*

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$ and assume both are primitive, in particular no prime integer divides all the a_j or all the b_j. Thus given any prime integer p, there is a smallest j so that p does not divide a_j and a smallest k so that p does not divide b_k. A calculation of the coefficient c_{j+k} of x^{j+k} in $f(x) * g(x)$ shows that p does not divide c_{j+k}. Since no prime divides all the coefficients of the product, the product is primitive.

The next theorem allows us to reduce factoring problems of integer polynomials to those of rational polynomials.

Theorem 5.2.5 *Let $f(x) \in \boldsymbol{Z}[x]$ and suppose in $\boldsymbol{Q}[x]$ $f(x)$ factors as $g(x) * h(x)$, i.e. $f(x) = g(x) * h(x)$ where $g(x), h(x) \in \boldsymbol{Q}[x]$. Then $f(x) = (c_g * c_h) * g^*(x) * h^*(x)$ where $g^*(x), h^*(x)$ are primitive polynomials in $\boldsymbol{Z}[x]$ and $c_g * c_h \in \boldsymbol{Z}$.*

Proof: By Gauss' Lemma $g^*(x) * h^*(x)$ is primitive so $c_g * c_h$ is the content of $f(x)$.

We can then deduce the unique factorization theorems and the greatest common divisor theorems from this.

Theorem 5.2.6 *Let $f(x) \in \boldsymbol{Z}[x]$, then $f(x)$ can be factored into a product of prime integers and primitive irreducible polynomials of degree ≥ 1, and this factorization is unique up to order of the factors and unit (± 1) multiples.*

In particular the *prime* elements of $\boldsymbol{Z}[x]$ are the prime integers and the primitive irreducible polynomials of degree ≥ 1. For example $f(x) = 36x^2 - 12x - 120$ factors as $f(x) = 2 * 2 * 3 * (3x - 5) * (x - 2)$. The polynomial $6x - 12$ would be irreducible, but would not be prime. The number 3 is a prime element of $\boldsymbol{Z}[x]$ but is not irreducible.

Theorem 5.2.7 *Given $f(x), h(x) \in \boldsymbol{Z}[x]$ there exists a greatest common divisor in the sense of Definition 1.8.1. In fact, if $g(x)$ is a greatest common divisor in $\boldsymbol{Q}[x]$ of $f(x)$ and $h(x)$ then in $\boldsymbol{Z}[x]$ $\gcd(f(x), h(x)) = \gcd(c_f, c_h) * g^*(x)$.*

5.3 Rational roots and factors

We start out with several simple theorems:

Theorem 5.3.1 *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial with integer coefficients, $a_n \neq 0$. Then if $g(x) = b_0 + b_1 x + \cdots + b_m x^m \in \boldsymbol{Z}[x]$ is a factor of $f(x)$ it must be that $b_0 | a_0$ and $b_m | a_n$.*

Proof: Use the formula for multiplication.

Theorem 5.3.2 *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \boldsymbol{Z}[x]$, $a_n \neq 0$, then the rational monic polynomial $g(x) = b_0 + b_1 x + \cdots + x_m$ is a factor of $f(x)$ in $\boldsymbol{Q}[x]$ only if $b_0 = c/d$ where $c, d \in \boldsymbol{Z}$ and $c | a_0$ and $d | a_n$, in fact, the least common multiple of all the denominators of the b_j (assuming all are in lowest terms) must divide a_n.*

Proof: $g*(x) = e*g(x) = (\frac{e}{d})c + eb_1x + \cdots + ex^m$ where e is the least common multiple of the denominators of the b_j (assuming in lowest terms) since the polynomial $g(x)$ is monic. Note $\frac{e}{d}$ is an integer. By 5.2.5 $g^*(x)$ divides $f(x)$, so 5.3.1 says that $e|a_n$ and $\frac{e}{d}c$ divides a_0 and hence c divides a_0.

Theorem 5.3.3 *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \boldsymbol{Z}[x]$ with $a_n \neq 0$. Any rational root is of the form c/d where $c, d \in \boldsymbol{Z}$ and $c|a_0, d|a_n$.*

Proof: Apply 5.3.2, recalling that c/d is a root if and only if $x - \frac{c}{d}$ is a factor.

For example, the polynomial $f(x) = 10x^3 - 5x + 12$ can have the possible rational roots $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12, \pm1/2, \pm3/2, \pm1/5, \pm2/5, \pm3/5, \pm4/5, \pm6/5, \pm12/5, \pm1/10, \pm3/10$ but in fact has none of them. Theorem 5.3.3 is widely overused as a method for finding roots to polynomials. This theorem should be used directly only when both a_0, a_n are ±1 or one is ±1 and the other is a prime number. In this case there are only a small number of possibilities. This theorem can be used after approximate roots have been found by calculator or computer. Then one can easily check and see if any of the roots are actually rational. In the example above the one real root is approximately -1.218523, which is clearly not one of the possible rational roots. It would have been a real waste of time to check each of the 32 possibilities.

While the previous two theorems are overused for finding linear factors, it is not widely known that they can be used effectively to find rational quadratic factors. If $f(x) = a_0 + a_1x + \cdots + a_nx^n$, a monic rational quadratic factor of $f(x)$ will be of the form

$$g(x) = x^2 + \frac{b}{d}x + \frac{c}{d}$$

where $c|a_0$ and $d|a_n$. If $z_1, z_2, \ldots, z_n$ are the complex roots of $f(x)$ (listed according to multiplicity) then two of them, say z_j, z_k will be roots of the quadratic factor $g(x)$. But then $z_j * z_k = c/d$ and $z_j + z_k = -b/d$ so one can fairly quickly check to see which pairs of roots can give rational factors. In particular, if z_j is an imaginary root it can only pair up with its conjugate and in this case $z_j * \overline{z_j} = |z_j|^2, z_j + \overline{z_j} = 2\text{Re}(z_j)$. The real roots can pair up in any way.

Example 5.3.4 Consider $f(x) = 3x^5 - 12x^4 + 16x^3 - 12x^2 + 3x + 6$. One finds, say

by ones TI-85 calculator, that the approximate roots are

$$\begin{aligned} z_1 &= .37004 + 1.091123i \\ z_2 &= .37004 - 1.091123i \\ z_3 &= 2.259921 \\ z_4 &= 1.457426 \\ z_5 &= -.457426 \end{aligned}$$

For two roots z_j, z_k to pair up to give a quadratic factor we must have $z_j + z_k = -b/d$ where $d = 1$ or 3 and $z_j * z_k = c/d$ where $d = 1$ or 3 and $c = \pm 1, \pm 2, \pm 3,$ or ± 6. But $2\text{Re}(z_1) = .74008$ which is not of this form so z_1, z_2 can be eliminated. Likewise $z_3 + z_4 = 3.717347$ and $z_3 + z_5 = 1.802494$ so these pairs are not possible. But $z_4 + z_5 = .999999$ is close enough to 1 to consider and $z_4 * z_5 = -.666666$ is also close to the allowable 2/3. Thus $g(x) = x^2 - x - 2/3$, or $g^*(x) = 3x^2 - 3x - 2$ are likely quadratic factors of $f(x)$. By division we check that these are indeed factors.

In theory one can also use Theorem 5.3.2 to look for cubic factors etc. however the number of combinations that may need to be checked is too large to be practical.

5.4 Eisenstein's Irreducibility Criterion

It would be nice to have a test for irreducible integer polynomials, but there is no simple general test. We will discuss some other tests later in the chapter but for now we mention one test that sometimes works.

Theorem 5.4.1 (Eisenstein's Irreducibility Criterion) *Let $f(x) = a_0 + a_1 x + \cdots + a_n x_n \in \boldsymbol{Z}[x]$ and p be a prime number. If p does not divide a_n, but p does divide $a_{n-1}, a_{n-2}, \ldots, a_0$ and p^2 does not divide a_0 then $f(x)$ is irreducible in $\boldsymbol{Z}[x]$.*

Proof: Let $f(x)$ satisfy Eisenstein's criterion and suppose $f(x) = g(x) * h(x)$ where $g(x), h(x) \in \boldsymbol{Z}[x], g(x) = b_0 + b_1 x + \cdots + b_m x^m$ and $h(x) = c_0 + c_1 x + \cdots + c_k x^k$. Now $a_0 = b_0 c_0$ is not divisible by p^2 so one of b_0, c_0 is not divisible by p, say b_0. But then c_0 is divisible by p, so pick the smallest index r such that c_r is not divisible by p (c_k cannot be divisible by p since a_n is not). Then $a_r = b_0 c_r + b_1 c_{r-1} + \cdots + b_r c_0$. But every term on the right is divisible by p except the first term $b_0 c_r$ and hence the right hand side is not divisible by p. Then a_r is not divisible by p so $r = n$ so $\deg h(x) = n$ and this says $f(x)$ is irreducible.

For example, Eisenstein's Criterion proves that the polynomial $x^5 - 6x + 3$ (of §4.10) is irreducible over $\boldsymbol{Z}[x]$, and hence also over $\boldsymbol{Q}[x]$.

Even though Eisenstein's criterion may not be directly applicable to some polynomials, it may still be used after a change of variables as the following easy theorem shows.

Theorem 5.4.2 *Let $f(x)$ be a rational or integer polynomial. Let $g(x) = b_0 + b_1(x - c) + \cdots + b_n(x - c)^n$. Then $f(x)$ is irreducible (over $\boldsymbol{Z}[x]$ or $\boldsymbol{Q}[x]$) if and only if $b_0 + b_1 y + \cdots + b_n y^n$ is.*

Example 5.4.3 Consider $f(x) = x^4 + x^3 + x^2 + x + 1$. This certainly does not satisfy Eisenstein's criterion, however expanding about $x = 1$ gives $f(x) = (x-1)^4 + 5(x-1)^3 + 10(x-1)^2 + 10(x-1) + 5$. But $y^4 + 5y^3 + 10y^2 + 10y + 5$ does satisfy Eisenstein's criterion for $p = 5$.

5.5 Hand Factoring Methods

In principle, integer polynomials can be factored in a finite number of steps. For example, the following theorem, which we state without proof, says that there are only finitely many possible factors and we could, in theory, try them all.

Theorem 5.5.1 *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be an integer polynomial. Let $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ be a factor of $f(x)$. Let $L = \sqrt{a_0^2 + a_1^2 + ... + a_n^2}$. Then $|b_j| \leq C(m, j)L$ where $C(m, j) = \frac{m!}{(m-j)!j!}$ is the binomial coefficient.*

Of course this bound can be quite large in practice. There are some slightly better methods, which are still impractical. For instance the method used in the last section for finding quadratic factors can be used for higher degree factors. We mention another method, attributed to Newton, only as an example of something that should **not** be tried. To find a factor of degree d, pick $d + 1$ distinct integers $x_0, x_1, \ldots, x_d$ and calculate $f(x_j) = y_j$ for $j = 0, \ldots, d$. Since $f(x)$ is an integer polynomial each y_j will be an integer. Now if $g(x) \in \boldsymbol{Z}[x]$ is a factor of $f(x)$ then $g(x_j)|y_j$ for each j. Thus every possible factor $g(x)$ of degree d can be obtained by taking factors $u_0, u_1, \ldots, u_d$ of $y_0, y_1, \ldots, y_d$ and using Lagrange interpolation to construct $g(x)$ so that $g(x_j) = u_j$ for each j.

We now suggest a strategy for factoring integer polynomials of small degrees which will certainly work for polynomials of degree 5 or less. This requires having a TI-85 or equivalent calculator which can find complex roots or an appropriate computer

program. It is interesting to note that whereas in high school factoring is taught as a method for finding roots, in real life it is usually done the other way around.

LET $f(x)$ BE OUR POLYNOMIAL, $\deg f(x) = n$.

1. FIND THE CONTENT OF $f(x)$, I.E. THE GCD OF ITS COEFFICIENTS. FACTOR THIS OUT.

2. CHECK TO SEE IF THERE IS A PRIME FOR WHICH EISENSTEIN'S CRITERION IS SATISFIED, I.E. CHECK THE PRIME FACTORS OF a_0. IF SO $f(x)$ IS IRREDUCIBLE AND YOU ARE DONE.

3. FIND APPROXIMATE REAL ROOTS FOR THE POLYNOMIAL AND CHECK AND SEE IF ANY OF THE ROOTS ARE RATIONAL. IF SO YOU HAVE A LINEAR FACTOR, WHICH CAN BE DIVIDED OUT TO GET A POLYNOMIAL OF SMALLER DEGREE. IF NOT, $f(x)$ IS IRREDUCIBLE IF $n \leq 3$, GO TO NEXT STEP IF $n > 3$.

4. FIND ALL ROOTS OF THE POLYNOMIAL AND USE THE METHOD GIVEN FOLLOWING THEOREM 5.3.3 TO LOOK FOR QUADRATIC FACTORS. DIVIDE OUT ANY QUADRATIC FACTORS FOUND. IF NO QUADRATIC FACTORS OR LINEAR FACTORS HAVE BEEN FOUND AND $n \leq 5$ THEN $f(x)$ IS IRREDUCIBLE.

Example 5.5.2 Let $f(x) = x^5 + x^4 + x^2 + x + 2$. $f(x)$ is primitive and $f(x)$ does not satisfy Eisenstein's criterion for $p = 2$, the only prime factor of a_0 so we go to step 3. Possible rational roots are $\pm 1, \pm 2$ but the only real root is -1.521380. The imaginary roots are $.760690 \pm .857874$ and $-.5 \pm .866025i$. The first conjugate pair does not give a rational factor but it is easily seen that the second conjugate pair are approximate roots of $x^2 + x + 1$ which is a factor. Dividing this out gives the other factor $x^3 - x + 2$. Since we have already determined that $f(x)$ has no linear factors this cubic must be irreducible. Thus the factorization of $f(x) = (x^2 + x + 1) * (x^3 - x + 2)$.

Exercise 5.5.1 (10 points each) Factor or prove irreducible using the methods of this section.

1. $x^5 + 28x^3 + 14x^2 - 21x + 35$

2. $x^4 + 2x^3 + 4x^2 + 4x + 7$

3. $162x^4 + 459x^3 + 81x^2 - 312x - 140$

4. $2x^5 + 5x^4 - 2x^3 - 3x^2 + 3x - 2$

If the method above does not work, say the degree is greater than 5, there are good factoring algorithms implemented in software such as MAPLE or MATHEMATICA. These will be briefly discussed in the next section.

A Comment on Integer Factoring in Elementary Mathematics Now that we have studied factoring over $\boldsymbol{Z}[x]$ and understand the difference between that and factoring over $\boldsymbol{R}[x]$ we might ask what should be role of factoring integer polynomials in math classes from algebra through calculus? It is integer factoring that is taught in high school algebra classes and this topic is often emphasized. Is this worthwhile?

In the opinion of your author, the answer is a qualified NO. Most uses of integer factoring in elementary mathematics are inappropriate, inefficient or both.

By inappropriate I mean that factoring in $\boldsymbol{Z}[x]$ is used in situations that call for factoring in $\boldsymbol{R}[x]$, or equivalently, root finding. By inefficient I mean that there are better algorithms for accomplishing the same thing.

Lets look at some of the applications of factoring in elementary math. The one that comes most readily is factoring to solve polynomial equations. Here integer factoring is both inappropriate and inefficient. Basically using integer factoring to solve equations is equivalent to guessing. There is nothing wrong with solving problems by guessing, but then why go to the trouble of mentioning factoring? In addition, as we showed in the example immediately after Theorem 5.3.3 this can be terribly inefficient. And of course, there is no reason to expect that typical problems give rational solutions. Besides, there are efficient methods for solving polynomial equations numerically, and in the case of quadratics a simple formula.

Here is a problem which is typical of an elementary algebra text which illustrates why I don't like factoring. *A rectangle has length 3 inches greater than the width and area 40 square inches. Find the length.* If we let x be the length then the width is $x-3$ so we have the equation

$$x(x-3)=40$$

Some re-arrangement gives the quadratic equation in standard form

$$x^2-3x-40=0$$

We can solve this by factoring, since the sign of the constant is negative we need two numbers whose product is 40 and difference is 3. But if we know two numbers whose product was 40 and difference was 3 we could have solved original problem immediately without doing any algebra at all. What have we taught the students? That algebra is useless?

Hopefully not. If the problem is changed just slightly, say the area of the rectangle is 50 sq. in. we now have a problem that requires the algebra to solve. But, of course, this

problem cannot be solved by factoring in $\boldsymbol{Z}[x]$. My contention is that by concentrating on problems that can be solved by factoring we lose the point of algebra.

Another problem that uses factoring is analyzing polynomial (usually quadratic) inequalities. But again factoring over $\boldsymbol{Z}[x]$ is inappropriate since we really want to factor over $\boldsymbol{R}[x]$. That is, we want to find the roots. The intermediate value theorem says the sign of the values of a polynomial function change only at the roots. Thus this problem should be approached by finding real roots and testing a point between the roots. This is a root finding, not a factoring problem.

What about integrating rational functions by partial fractions decomposition? Certainly this requires factoring. But the point of D'Alembert's Theorem is that this is factoring over $\boldsymbol{R}[x]$. Besides, with numerical algorithms for integrating on our calculators, and computer algebra integrating routines, who integrates messy functions by hand anymore anyway?

But, you say, how can one simplify a rational expression such as

$$\frac{x^2 + x - 6}{x^2 + 4x + 3}$$

without factoring? Well, how about subtracting the numerator from the denominator? You get $3x + 9$ which is 3 times the common factor $(x + 3)$. A coincidence? Not really. The common factor of numerator and denominator is the greatest common divisor of them. Finding gcd's is much simpler than factoring, usually.

The above being said, factoring in $\boldsymbol{Z}[x]$ is an interesting problem, part of the culture of mathematics, and probably helps students learn facility with algebraic computations. It would be wrong to ban it from the curriculum. But on the other hand we should not overemphasize it either as a skill or a problem solving tool.

5.6 Computer Factoring

The problem of computer factoring integer polynomials, and polynomials with coefficients in certain more complicated integral domains, is of interest to number theorists and computer scientists. As a result algorithms have been developed.

A fairly simple way to factor integer polynomials, but not the most efficient, is, as in hand factorization, to find a root, preferably imaginary, and then look for the minimimal polynomial which will be an irreducible factor. One can use, for example, the Maple procedures described in §5.1 to look for minimal polynomials of degrees less than the original polynomial and then use the division algorithm to check that the polynomials

given are actually factors. This will usually work well, but in some cases not, so failure by this method is not conclusive proof that the original polynomial is irreducible.

Most computer methods, however, first factor over fields of modular arithmetic. The mod function $r = b \bmod m$ finds the remainder r when integer b is divided by positive integer m using the division algorithm for integers. If one fixes a prime number p then addition and multiplication can be defined on the set $\boldsymbol{Z}_p = \{0, 1, 2, \ldots, p-1\}$ by

$$a + b = (a + b) \bmod p$$
$$a * b = (ab) \bmod p$$

The resulting algebraic system actually satisfies the field axioms of section 1.1. There are some technical details that must be dealt with, for example polynomials cannot be viewed as functions, but basically the ring $\boldsymbol{Z}_p[x]$ behaves similarly to the ring of polynomials over any field we have studied, including a unique factorization theorem. A more thorough discussion of this is contained in earlier versions of these notes, which may still be available from my website.

In $\boldsymbol{Z}_p[x]$ factorization is a finite process that can be done efficiently by computer. The two main algorithms used are the distinct-degree algorithm and Berlekamp's algorithm. The distinct degree algorithm, discussed in earlier editions of these notes, uses the somewhat bizarre fact, not proved in the notes, that the polynomial $x^{p^d} - x$ has every irreducible polynomial of degree d as a factor. Thus, in principle, all one needs to do is take the greatest common divisor of the polynomial of degree n to be factored with these polynomials for $d \leq n/2$. The actual algorithm uses other strange facts about modular polynomials to make this efficient. Berlekamp's algorithm is more complicated, using linear algebra as well as number theory. Berlekamp's algorithm is usually reserved for the case where p is large and the polynomial has few factors.

Maple Implementation

Maple implements both the distinct-degree and Berlekamp's algorithm. Enter a polynomial f with variable x, in the usual manner, but with integer coefficients, select a prime p and then use

```
DistDeg(f,x) mod p;
       or
Berlekamp(f,x) mod p;
```

Note that `DistDeg` will return pairs $[g, d]$ where g is a not-necessarily irreducible factor which is a product of irreducibles of degree d. Berlekamp will attempt to return a complete factorization.

One use of factoring over $\boldsymbol{Z}_p[x]$ is that one can often obtain proofs that a given polynomial in $\boldsymbol{Z}[x]$ is irreducible. For example if f is irreducible in $\boldsymbol{Z}_p[x]$ for some then it must have already been irreducible in $\boldsymbol{Z}[x]$. The converse is not true, but by trying various primes p one can find a suitable one or argue indirectly if the factorizations over different p are incompatible.

Maple, and other factoring software, use information gathered from factorization over $\boldsymbol{Z}_p[x]$ to give clues on factoring in $\boldsymbol{Z}[x]$. For example, Maple uses distinct-degree factorization as part of its `factor` algorithm. In general Maple is successful at factoring most "reasonable" integer polynomials.

Maple Implementation

To factor an integer or rational polynomial simply use

```
factor(f)
```

Note that you do not specify the variable as Maple will factor anything in sight, separating, if possible, the different variables.

5.7 Comparison of factoring algorithms

As mentioned in §2.2 the two concerns we have about algorithms are accuracy and efficiency. For factoring, accuracy is not a concern – one can test supposed factors and they work or don't work. Efficiency is a concern in factoring. For both integers and polynomials there are simple algorithms that will work, the problem is to find algorithms that work quickly.

For example, in factoring an integer N one procedure, we will call this "straight factoring" is to divide N first by 2 and then by each odd integer $3, 5, 7, 9, \ldots$ up to $\sqrt{N}$ looking for factors. With a computer or programmable calculator this is as quick as almost any algorithm for small integers, say integers less than 1,000,000. However for each two digits added to N the time taken will be multiplied by $\sqrt{100} = 10$. Thus if our computer takes 5 seconds to factor a 6 digit number by the straight factor method it will take 100 years to factor a 30 digit number by this method! We want an algorithm which will give us an answer today, not 100 years from today.

In calculating the time to be taken by a factoring method we use as the "size" of an integer its number of digits. For a polynomial with integer coefficients we use the degree and the number of digits in the coefficients. Since it takes longer to add, multiply and divide longer integers, this has to be considered in calculating the efficiency. The efficiency, or *complexity* of an algorithm will then be a function of its size.

In calcuating the efficiency of an algorithm we generally ignore constant multiples or constants added. For instance, it makes little difference to us if it takes 100 years or 200 years to factor our 30 digit number – in either case we won't be alive to see the results. Besides it is always possible to obtain a computer which operates twice as fast, or, as is often done, to use many computers. Thus we make the following definition.

Let r, s be real valued functions defined on the non- negative integers $0, 1, 2, \ldots$ r is said to be $O(s)$ (read *big Oh of* s) if there exist constants k and M so that for all $n \geq k, r(n) < Ms(n)$. For further discussion of this idea, see almost any text on discrete mathematics or theory of algorithms.

It is not hard to see that if $r(n)$ is a polynomial in n of degree d then r is $O(n^d)$. Any algorithm that has a complexity of $O(n^d)$ for some d is called a *polynomial time* algorithm and a problem with a polynomial time algorithm is called *tractable*. For example, the straight factor algorithm has complexity $O(10^{N/2})$ which is not polynomial time. A tractable algorithm is considered acceptable by people who worry about speed of algorithms.

It is still an important open question in mathematics as to whether there is an algorithm for factoring integers in polynomial time. There are algorithms far better than straight factor, but it still takes 1 month to factor a 100 digit number. It is widely suspected that the problem of factoring integers is *intractible*.

Factoring polynomials is a different story. In 1984, Lenstra, Lenstra and Lovasz discovered that by factoring over $\boldsymbol{Z}_p$ for suitable p using Berlekamps algorithm, by applying something called Hensel Lifting to get a factorization over the ring $\boldsymbol{Z}/p^e$, for suitable e, and finally applying the Basis Reduction algorithm discussed above to get a factorization over $\boldsymbol{Z}[x]$ then one can factor polynomials in time $O(n^{10} + Mn^8)$ where M is a function of the size of the coefficients and n is the degree of the polynomial. In particular, the problem of factoring polynomials is tractable. The article by Susan Landau is slightly out of date but a good survey article on this subject. Thus it appears to us today that factoring polynomials is a considerably easier problem than factoring integers!

Example 5.7.1 Would you rather factor the integer 1945448129 or the polynomial $x^2 - 89454x + 1945448129$? I would pick the latter, for using even an ordinary calculator I could easily get an approximate root by the quadratic formula. (Hint: if your calculator only is accurate to, say, 8 digits, use the transformation $1000y = x$ to get $1000000y^2 - 89454000y + 1945448129 = 0$ and divide by 1000000 to get the easily solved quadratic $y^2 - 89.454y + 1945.448 = 0$. Multiply the answer by 1000 to get x.) If this quadratic factors over $\boldsymbol{Z}[x]$ it has an integer root which I could find by rounding my approximate root and then I could easily factor the quadratic. On the other hand factoring this 11

digit integer directly would not be easy (try it!). For example, straight factor on my TI-85 took over 23 minutes. The point is, of course, that the coefficient of x in the quadratic gives me enough extra information to make my job much easier.