Parabola Volume 38, Issue 2 (2002)

COMPUTERS AND POLYNOMIALS

John D. Steele [1]

Introduction

In an earlier article (*Parabola*, 37(3), (2001), 7-11) I talked about **computer algebra systems**: software packages that, as the name suggests, do algebra. In that article I looked at how such packages cope with arithmetic to unlimited precision. In this article I want to look at the algebra side of the packages, in particular polynomials.

The basic problem with polynomials is factorization: writing a polynomial as the product of polynomials of smaller degree, where possible. Remember that the **degree** of a polynomial is the highest power that occurs: the coefficient of the highest power is called the **leading coefficient**. Many polynomials that one deals with have coefficients that are integers, and we are after a factorization into factors that also have integer coefficients — we call this a **factorization over the integers**.

The general method used by computer algebra systems to factorize polynomials would take too long to detail here, although it does not require advanced mathematics — basic polynomial arithmetic and the ability to solve systems of simultaneous linear equations is all that is required. The key process, which is used to do integration, among other things is based on the idea of **modular arithmetic**.

Modular Arithmetic

Modular arithmetic is the name given to arithmetic with remainders after division — I touched on this idea in my previous article. We use this type of arithmetic in everyday life, in fact whenever we tell the time. If it is 10 o'clock and I'm going to do something that takes 4 hours, then I expect to finish not at 14 o'clock but at 2 o'clock: 2 is the remainder on dividing 14 by 12. We call this **arithmetic modulo 12**. With the clock we talk about 12 o'clock rather than zero o'clock, but in mathematics we would usually use the numbers 0, 1, 2 . . . 11 for the remainders.

It turns out that arithmetic modulo 12 is not very useful. It is better to consider arithmetic modulo a prime, such as 3, 5 or 7 — or even 2 in some cases. In computer algebra systems we also prefer to use positive and negative remainders. So for arithmetic modulo 5 we would be working with the numbers -2, -1, 0, 1 and 2.

As an example, in arithmetic modulo 7, $6^2 = (-1)^2 = 1$ and $5^2 = -3$.

Roots of Polynomials

[1] John Steele is a Lecturer in Pure Mathematics at UNSW

One of the results you will have learned about polynomials is that roots (where the polynomial has value zero) and linear factors are intimately related. The **Factor Theorem** says that for a polynomial $f(x)$, if $f(a) = 0$ then we can write $f(x) = (x - a)q(x)$ for some polynomial $q(x)$ of smaller degree than $f(x)$. If we want to find a linear factor with integer coefficients, then we need to look at all possible *rational* roots of the polynomial. For example, $2x^2 - x - 6$ has two roots, 2 and $-\frac{3}{2}$, and so factorizes as $2(x + \frac{3}{2})(x - 2) = (2x + 3)(x - 2)$.

Now in looking for rational roots of an integer polynomial you do not need to check every rational. You may also know the result: that if the rational number p/q (in lowest terms) is a root of the polynomial $f(x)$, then p divides the constant term and q divides the leading coefficient. So for $2x^2 - x - 6$, there are four divisors of the constant term (1, 2, 3 and 6) and two of the leading coefficient (1 and 2) — we ignore signs for the moment — and we find 6 possible positive rational roots: 1, 2, 3, 6, $\frac{1}{2}$ and $\frac{3}{2}$. Double this number to account for the sign and we have to check 12 possible rational numbers to get a rational root, and therefore an integer factor.

That example is not too bad, but consider the polynomial $p(x) = 72x^3 - 99x^2 - 85x - 86$. To check for a rational root, you need to look at all rational numbers of the form (divisor of 86)/(divisor of 72), and there are 60 possibilities for this.

What we want is a quicker way.

Factorizing Modulo a Prime

We make use of the idea of modular arithmetic to speed up the hunt for integer factors. The Factor Theorem is still true when we do all the arithmetic modulo any integer, and it is also easy to see that a factorization over the integers **descends** to a factorization modulo any prime (or any integer). What I mean by this is that if we have $f(x) = g(x)h(x)$ with integer coefficient polynomials, then we can take each coefficient modulo any prime p we like and get a correct factorization modulo p. So as

$$2x^4 + 13x^3 + 12x^2 - 29x - 14 = (2x^2 + 3x - 7)(x^2 + 5x + 2)$$

over the integers, then modulo 5

$$2x^4 - 2x^3 + 2x^2 + x + 1 = (2x^2 - 2x - 2)(x^2 + 2).$$

This is the key point of the method that computer algebra systems use to factorize polynomials.

Unfortunately, while factorizations descend they do not always ascend. It is possible that a polynomial can be factorized modulo a certain prime but not factorized over the integers. In fact, there are polynomials (infinitely many in fact) that can be factorized modulo *every* prime but not over the integers. One of the simplest is $x^4 + 1$ which has no real roots at all, but is $(x + 1)^4$ modulo 2, $(x^2 - x - 1)(x^2 + x - 1)$ modulo 3, $(x^2 - 2)(x^2 + 2)$ modulo 5 and so on.

There are methods that computer algebra system can use to get around this fact, but I'll not discuss them here. However, a simple consequence of the descent of factorizations is that if a polynomial has no factors modulo a particular prime, then it has

no factorization over the integers (if it did, that factorization would descend). So, if we can find a prime p for which polynomial $f(x)$ has no factors, then $f(x)$ is **irreducible over the integers**, that is, it has no integer factors.

Irreducible Polynomials

What primes ought we to look at to prove irreducibility? Firstly, it is clear that any prime that divides the constant term is no use: when we take the polynomial modulo such a prime then there is no constant term and so 0 is a root modulo the prime. We can also ignore primes that divide the leading coefficient, as then taking the polynomial modulo such a prime will give us a polynomial of smaller degree than we started with.

We will concentrate on the existence of linear integer factors, which by the factor theorem is the same as looking for rational roots. Recall that a quadratic or cubic is irreducible over the integers if and only if it has no rational roots, so this is all we need to do for such polynomials.

Consider the example $f(x) = x^2 + 2x + 3$. This factors modulo 2, as it becomes $x^2 + 1 = (x + 1)^2$ modulo 2. We ignore 3 as that divides the constant term. For prime 5 we need to check only the 5 numbers -2, -1, 0, 1 and 2. Clearly $f(0) = 3 \neq 0$ and we also get $f(\pm 1) = 1 \pm 2 + 3 \neq 0$ and $f(\pm 2) = 4 \pm 4 + 3 \neq 0$, so $f(x)$ has no roots modulo 5 and hence no integer factors.

You might not be too impressed with this example, as it is easy to check the 4 possible rational roots of $f(x)$ (± 1, ± 3) by hand. But the above calculation also proves that $16x^2 - 17x + 33$ has no integer factors, as it is the same polynomial as $f(x)$ when taken modulo 5, and there are 40 possible rational roots to check for this polynomial.

As a further example, in the 2001 HSC Mathematics Extension 2 ("4-Unit") paper one of the questions asked to prove that the polynomial $x^3 - 3x + 1$ had no rational roots. This is an easy exercise using the result about divisors mentioned above (the full question involved proving that result), and we can use modular arithmetic to get this too: modulo 2 the polynomial is just $x^3 + x + 1$, which has neither 0 nor 1 as a root modulo 2.

Let us now look at the polynomial $p(x) = 72x^3 - 99x^2 - 85x - 86$ mentioned earlier. We can prove this has no integer factors without checking 60 possibilities, but only 5. We again choose prime 5, as 2 and 3 divide the leading coefficient. Modulo 5 we have $p(x) = 2x^3 + x^2 - 1$, so $p(0) = -1$, $p(1) = 2 + 1 - 1 = 2$, $p(-1) = -2 + 1 - 1 = -2$, $p(2) = 2 \times 8 + 4 - 1 = 1 - 1 - 1 = -1$ modulo 5, and $p(-2) = -2 \times 8 + 4 - 1 = -1 - 1 - 1 = 2$ modulo 5. So $p(x)$ has no roots modulo 5 and hence no integer linear factors and thus is irreducible over the integers.

WEB HIGHLIGHTS

http://www.austms.org.au/

The web site for the Australian Mathematics Society is an excellent starting point for students interested in finding out about the diverse range of careers and job opportunities in mathematics.