Modern Algebra + Number Theory + Analysis:
Factoring in $\mathbb{Z}[x]$ via Lagrange Interpolation

Factoring is a concept that runs throughout the mathematics curriculum in a number of forms as a topic from beginning algebra to advanced mathematics. We will combine concepts from Modern Algebra, Number Theory, and Analysis to generate an algorithm for factoring polynomials. First, we define our terms.

**Definition 1 (Polynomials over $\mathbb{Z}$).** Let $x$ be an indeterminate. Define $\mathbb{Z}[x] = \{ p(x) | p$ is a polynomial in $x$ with coefficients from $\mathbb{Z} \}$

A natural question is is using $\mathbb{Z}$ rather than $\mathbb{Q}$ too restrictive? Since we can easily calculate the lcm of the set of denominators of the coefficients from $q(x) \in \mathbb{Q}[x]$, we can multiply by the lcm to generate a polynomial $z(x) \in \mathbb{Z}[x]$. Then

$q(x) = \frac{1}{\text{lcm}} z(x)$

Thus factoring $z$ factors $q$ and vice versa.

**Analysis**

*Lagrange Interpolation* is a technique from Approximation Theory, a branch of Analysis. The Lagrange interpolating polynomial $L_n$ is an $n$th degree polynomial that passes through $(n + 1)$ given data points. Let $K = \{ x_0 < x_1 < \cdots < x_n \}$ be a collection of $n + 1$ $x$-values called knots.

**Definition 2 (Fundamental Lagrange Polynomial).** Given a set of $n + 1$ knots $K$, define the Fundamental Lagrange Polynomials $l_k(x)$ by

$$l_k(x) = \frac{x - x_0}{x_k - x_0} \times \frac{x - x_1}{x_k - x_1} \times \cdots \times \frac{x - x_{k-1}}{x_k - x_{k-1}} \times \frac{x - x_{k+1}}{x_k - x_{k+1}} \times \cdots \times \frac{x - x_n}{x_k - x_n} = \prod_{j=0}^{n} \frac{x - x_j}{x_k - x_j}$$

for $k = 0..n$.

We immediate see that

**Proposition 1.** For a set $K$ of knots $\{ x_j \}$, the fundamental Lagrange polynomial satisfies

$$l_k(x_j) = \delta_{j,k};$$

i.e., $l_k(x_k) = 1$ and, if $j \neq k$, then $l_k(x_j) = 0$.

*Proof.* Exercise. Simple computation.

The above result lets us easily construct an $n$th degree polynomial passing through $n + 1$ data points. This polynomial is called the *Lagrange Interpolating polynomial*.

**Proposition 2.** Let $K$ be a set of knots and $Y = \{ y_0, y_1, \ldots, y_n \}$ be the associated $y$-values. Then the polynomial

$$L_n(x) = \sum_{k=0}^{n} y_k \cdot l_k(x)$$

has degree $n$ and satisfies $y_j = L_n(x_j)$ for $j = 0..n$.

*Proof.* Exercise. Simple computation.
Example 1. Find a cubic polynomial that goes through the points $(0, 1), (3, 1), (13/4, 0),$ and $(4, 0)$.

Solution. Using the proposition above, we see that

\[ L_3(x) = 1 \cdot \frac{(x - 3)(x - 13/4)(x - 4)}{(0 - 3)(0 - 13/4)(0 - 4)} + 1 \cdot \frac{(x - 0)(x - 13/4)(x - 4)}{(3 - 0)(3 - 13/4)(3 - 4)} + 0 \cdot \frac{(x - 0)(x - 3)(x - 4)}{(13/4 - 0)(13/4 - 3)(13/4 - 4)} + 0 \cdot \frac{(x - 0)(x - 3)(x - 13/4)}{(4 - 0)(4 - 3)(4 - 13/4)} \]

\[ = \frac{17}{13} x^3 - \frac{489}{52} x^2 + \frac{855}{52} x + 1 \]

Note how much the polynomial oscillates to reach all the data.

Number Theory

The Chinese Remainder Theorem is an important result from Number Theory that has been known for nearly two thousand years. The Chinese mathematician Sun Tzu\textsuperscript{1} gave the theorem in his 3rd century text *Sun Tzu Suan Ching* (Sun Tzu’s Calculation Classic). As a proposition in Number Theory, the theorem is stated as:

**Theorem 3** (Chinese Remainder Theorem). Let $\{n_1, n_2, \ldots, n_j\}$ be a set of pairwise relatively prime integers. For any set $\{a_1, a_2, \ldots, a_j\}$ of integers, there exists a solution of the system of congruence equations

\[ x \equiv a_1 \pmod{n_1} \]
\[ x \equiv a_2 \pmod{n_2} \]
\[ \vdots \]
\[ x \equiv a_j \pmod{n_j}. \]

Further, all solutions are congruent modulo $N = \prod n_j$.

**Proof.** A clever sequence of substitutions using the fact $x \equiv a_i \pmod{n_i} \iff x = k n_i + b_i$ builds the solution. \hfill \Box

**Alternate proof.** Set $N_i = N/n_i$ for each $i = 1..j$. Since $N_i$ and $n_i$ are relatively prime, we can solve each of the congruences $N_i y_i \equiv 1 \pmod{n_i}$. Call the solution $y_i$.

Exercise: Show that

\[ x \equiv \sum_{i=1}^{j} a_i N_i y_i \]

solves each congruence. \hfill \Box

---

\textsuperscript{1}The mathematician Sun Tzu is not the same Sun Tzu who wrote *The Art of War* 800 years earlier. Tzu \textsuperscript{2}“Master.”

\textsuperscript{2}A problem in Sun Tzu’s text: There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?
Algorithm 1 (Factoring by Interpolation). Let \( p(x) \in \mathbb{Z}[x] \) with degree \( n \). If \( p \) has any factors, then the degree of one factor must be less than or equal to \( d = \lfloor n/2 \rfloor \).

1. Choose \( d + 1 \) distinct integers \( v_0, v_1, \ldots, v_d \) and set \( v_0 = p(0) \). Define the vector \( \mathbf{v} = [v_0, v_1, \ldots, v_d] \) formed above. Use either Langrange interpolation or the Chinese Remainder Theorem to generate the polynomials.

2. List every vector of the form \( \mathbf{v} = [v_0, v_1, \ldots, v_d] \) where \( s \) is a factor of \( p \). For example, if \( p = 6 \), then \( v_0 = 1, -1, \) or \( \pm 2 \).

3. For each vector \( \mathbf{v} \), form the polynomials \( L_i \) for \( i = 0, 1, \ldots, d \) such that \( L_i(x) = \frac{(x - v_0)(x - v_1)\cdots(x - v_{i-1})(x - v_{i+1})\cdots(x - v_d)}{(v_i - v_0)(v_i - v_1)\cdots(v_i - v_{i-1})(v_i - v_{i+1})\cdots(v_i - v_d)} \).

4. Test each polynomial \( L_i \) to see if it is a factor of \( p \).

The Project

We continue by proving Theorem 4 (The Chinese Remainder Theorem for Polynomials). Let \( F \) be a field. Let \( a_1(x), a_2(x), \ldots, a_t(x) \) be polynomials in \( F \) and let \( b_1, b_2, \ldots, b_t \) be a collection of mutually relatively prime polynomials in \( F \). Then there is a polynomial \( p \in F \) that solves each congruence \( p(x) \equiv a_i(x) \pmod{b_i} \). Theorem 4 shows that the solution \( p(x) \) is unique up to a constant factor. The proof is similar to the proof of the Chinese Remainder Theorem for numbers. We present it here for completeness.

Algorithm 2

1. Choose \( 1 \) distinct integers \( v_0 = 0, v_1, \ldots, v_d \).
2. Choose \( d + 1 \) distinct integers \( b_0 = 1, b_1, \ldots, b_n \)
3. Choose \( s \) distinct integers \( s_0 = 0, s_1, \ldots, s_n \).
4. Test each polynomial \( L_i \) to see if it is a factor of \( p \).

Corollary 5

Let \( p \in F \) and \( b \in F \). Then \( h(x) = b \cdot (x - a) \) if and only if \( p(a) = 0 \).

Further, \( g(x) \) is also a solution if and only if \( f(x) \equiv g(x) \pmod{b(x)} \).

Example 2

Solve Sun Tzu's problem:

\[
\begin{align*}
1. \quad & 7 \equiv 2 \pmod{3} \\
2. \quad & 5 \equiv 3 \pmod{7} \\
3. \quad & 5 \equiv 2 \pmod{5} \\
4. \quad & 7 \equiv 3 \pmod{8} \\
\end{align*}
\]

Solution. An \( x \) that satisfies the first congruence has form \( x = 3a + 2 \) for some integer \( a \). Substitute this value into the second congruence to have \( 3a + 2 \equiv 1 \pmod{5} \). Thus \( a = 2, 7, \) and so \( x = 8, 15 \). Now put this value into the third congruence to have \( 5 \equiv 1 \pmod{8} \) or \( x = 3, 5, 7, \) or \( x = 11, 19 \). Hence, our solution is \( x = 23, 128, 233 \ldots \). Note that \( 105 \equiv 1 \pmod{20} \).
Problem 1. Factor the following polynomials using the algorithm:

1. Factor \( p(x) = x^4 - x^2 - 2x - 1 \). Use knots \([0, 1, -1]\).

2. Factor \( r(x) = x^5 + x + 1 \).

3. Factor \( \psi(x) = x^6 + 3x^4 + 2x^3 + 2x^2 + 3x + 1 \).

(Hint: Look at the Maple worksheet.)

Project Report

Your project report should contain:

- Your and your partners names at the top right of the first page.
- Carefully crafted proofs and the results of the problems for Algorithm 1.
- A narrative connecting the propositions together.

Your project grade will be based on both your results and your writing.

Extras

Lagrange was a protégé of Euler and the advisor of Fourier. W. W. Rouse Ball states in A Short Account of the History of Mathematics that Lagrange was “greatest mathematician of the eighteenth century.” See his biography at the MacTutor math history web site.

Chapter 1, page 1, of Sun Tzu Suan Ching (Sunzi suanjing) c. 400 AD (?)

Almost nothing in known of Sun Tzu (also called Sun Zi) or his life. Even the date of his book is uncertain and based on indirect evidence.

To The Future Teacher

What does the textbook problem “Factor \( x^2 - 9 \) completely.” mean? For example, we see that \( x^4 - 9 \) factors as \((x^2 + 3)(x^2 - 3)\) over the integers, but as \((x^2 + 3)(x + \sqrt{3})(x - \sqrt{3})\) over the real numbers. Further, \( x^2 - 9 \) can be factored as \((x + i\sqrt{3})(x - i\sqrt{3})(x + \sqrt{3})(x - \sqrt{3})\) over \( \mathbb{C} \). Much more complicated examples can be easily found in rings like \( \mathbb{Q} [\sqrt{2}] \).

Even though you won’t use the terms field and ring in an Elementary Algebra class, they are critical to your understanding so that you can help your students learn “how to factor.” You will have to think carefully how you will explain to your students at different levels whether a polynomial ‘factors’ or not.