Computational Models of Mathematical Systems

Al Cuoco
Center for Mathematics Education, EDC

for
Wally Feurzeig

Joint Mathematics Meetings, January 2013

Learning transforms lives.

Outline

1. Getting Started
   - Experience with Technology
   - The Physics of Mathematics
2. The Mathematics
   - Cyclotomic Integers
   - Splitting Fields
3. The Model
   - A universal modeling method
   - Taking it out for a spin
4. Parting Thoughts and Thanks
   - Some Thoughts and Conclusions

Outline

From MET-II

- Teachers should become familiar with various software programs and technology platforms, learning how to use them to analyze data, to reduce computational overhead, to build computational models of mathematical objects, and to perform mathematical experiments.

- The experiences should include dynamic geometry environments, computer algebra systems, and statistical software, *used both to apply what students know and as tools to help them understand new mathematical ideas*—in college, and in high school.

From MET-II

- *Not only can the proper use of technology make complex ideas tractable, it can also help one understand subtle mathematical concepts.*
- At the same time, technology used in a superficial way, without connection to mathematical reasoning, can take up precious course time without advancing learning.

Outline

EDC Learning transforms lives.

Mathematical Imagery

- Think of the way you envision polynomial multiplication, or the changing shape of a rectangle as it maintains a constant area.

Mathematical Imagery

- Think of the way you envision polynomial multiplication, or the changing shape of a rectangle as it maintains a constant area.
- What do you see when you think of counting the number of factors in an integer?

Mathematical Imagery

- Think of the way you envision polynomial multiplication, or the changing shape of a rectangle as it maintains a constant area.
- What do you see when you think of counting the number of factors in an integer?

Riemann visualized functions as liquids flowing over surfaces, and Kummer talked about “ghost factors.” There are hundreds of similar examples of mental images people use when thinking about mathematics.

A *CME* Conjecture

- Greater opportunities to tinker with mathematical objects, just as they might tinker with mechanical objects, will allow more students to develop a sense for the physics of mathematics.

A *CME* Conjecture

- Greater opportunities to tinker with mathematical objects, just as they might tinker with mechanical objects, will allow more students to develop a sense for the physics of mathematics.

- But mathematical objects are objects of the imagination, and many don't have physical models. How, then, can people tinker with these systems or the mathematical objects of which they're built?

Enter Technology

- They may not have physical models, but they *do* have computational models.
- By building computational models for mathematical objects and processes, students construct corresponding mental models that translate into new knowledge.

Outline

EDC Learning transforms lives.

Roots of Unity

If n is a positive integer,

$$\begin{aligned} x^n - 1 &= (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1\right) \\ &= (x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^3)\ldots(x-\zeta^{n-1}) \end{aligned}$$

where

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

Roots of Unity

If n is a positive integer,

$$
\begin{aligned}
x^n - 1 &= (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1\right) \\
&= (x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^3)\ldots(x-\zeta^{n-1})
\end{aligned}
$$

where

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

$\mathbb{Z}[\zeta]$ is called the *ring of cyclotomic integers*.

EXAMPLE: $n = 4$

$$
\begin{aligned}
x^4 - 1 &= (x-1)(x^3 + x^2 + x + 1) \\
&= (x-1)(x-i)(x-i^2)(x-i^3)
\end{aligned}
$$

$\mathbb{Z}[i]$ is called the ring of *Gaussian integers*.

EXAMPLE: $n = 3$

$$\begin{aligned} x^3 - 1 &= (x-1)(x^2+x+1) \\ &= (x-1)(x-\omega)(x-\omega^2) \end{aligned}$$

where $\omega = \frac{-1+i\sqrt{3}}{2}$

$\mathbb{Z}[\omega]$ is called the ring of *Eisenstein integers*.

EISENSTEIN INTEGERS

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

Eisenstein Integers

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

In $\mathbb{Z}[\omega]$,

- $$\overline{\omega} = \omega^2 = \frac{1}{\omega} = \frac{-1 - i\sqrt{3}}{2}$$
- If $z = a + b\omega$

$$N(\omega) = \omega\,\overline{\omega} = a^2 - ab + b^2$$

Eisenstein Integers

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

In $\mathbb{Z}[\omega]$,

- $$\overline{\omega} = \omega^2 = \frac{1}{\omega} = \frac{-1 - i\sqrt{3}}{2}$$
- If $z = a + b\omega$
$$N(\omega) = \omega\,\overline{\omega} = a^2 - ab + b^2$$

Eisenstein integers have all kind of applications:

Eisenstein Integers

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

In $\mathbb{Z}[\omega]$,

- $$\overline{\omega} = \omega^2 = \frac{1}{\omega} = \frac{-1 - i\sqrt{3}}{2}$$
- If $z = a + b\omega$

$$N(\omega) = \omega\,\overline{\omega} = a^2 - ab + b^2$$

Eisenstein integers have all kind of applications:

- Proving Fermat's Last Theorem for exponent 3.

Eisenstein Integers

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

In $\mathbb{Z}[\omega]$,

- $$\overline{\omega} = \omega^2 = \frac{1}{\omega} = \frac{-1 - i\sqrt{3}}{2}$$
- If $z = a + b\omega$

$$N(\omega) = \omega\,\overline{\omega} = a^2 - ab + b^2$$

Eisenstein integers have all kind of applications:

- Proving Fermat's Last Theorem for exponent 3.
- Making up problems that come out nice.

EDC Learning transforms lives.

An authoring tool becomes a teaching tool

- The need to make up problems involving $\mathbb{Z}[\omega]$ led to the need for a computational model of this ring.

An authoring tool becomes a teaching tool

- The need to make up problems involving $\mathbb{Z}[\omega]$ led to the need for a computational model of this ring.
- The model used a classical theorem of Kronecker as the basic engine.

An authoring tool becomes a teaching tool

- The need to make up problems involving $\mathbb{Z}[\omega]$ led to the need for a computational model of this ring.
- The model used a classical theorem of Kronecker as the basic engine.
- And building the model was a worthwhile exercise on its own.

Outline

Constructing a home for a root

Theorem (Kronecker): Let k be a field, let $p(x) \in k[x]$ be a monic irreducible polynomial.

- $K = k[x]/(p(x))$ is a field and k is (isomorphic to) a subfield of K.
- The congruence class of x is a root of p in K.

Constructing a home for a root

Theorem (Kronecker): Let k be a field, let $p(x) \in k[x]$ be a monic irreducible polynomial.

- $K = k[x]/(p(x))$ is a field and k is (isomorphic to) a subfield of K.
- The congruence class of x is a root of p in K.

Hence $\mathbb{Q}[\omega]$ can be realized as $\mathbb{Q}[x]/(x^2 + x + 1)$.

Constructing a home for a root

Theorem (Kronecker): Let k be a field, let $p(x) \in k[x]$ be a monic irreducible polynomial.

- $K = k[x]/(p(x))$ is a field and k is (isomorphic to) a subfield of K.
- The congruence class of x is a root of p in K.

Hence $\mathbb{Q}[\omega]$ can be realized as $\mathbb{Q}[x]/(x^2 + x + 1)$.

And the Eisenstein integers can be modeled as using elements of $\mathbb{Q}[x]$ with integer coefficients.

Outline

Components of the Model

We want to build a model of "polynomials mod $x^2 + x + 1$."

Components of the Model

We want to build a model of "polynomials mod $x^2 + x + 1$."

- A universal method for modeling mathematical systems is developed in *Structure and Interpretation of Computer Programs* (Abelson-Sussman).

Components of the Model

We want to build a model of "polynomials mod $x^2 + x + 1$."

- A universal method for modeling mathematical systems is developed in *Structure and Interpretation of Computer Programs* (Abelson-Sussman).
- In our case, the elements are congruence classes modulo $x^2 + x + 1$.

Components of the Model

We want to build a model of "polynomials mod $x^2 + x + 1$."

- A universal method for modeling mathematical systems is developed in *Structure and Interpretation of Computer Programs* (Abelson-Sussman).
- In our case, the elements are congruence classes modulo $x^2 + x + 1$.
- The operations are
  - Addition and multiplication
  - Conjugation
  - Norm and division (in $\mathbb{Q}[\omega]$)

Scratchpad

EDC Learning transforms lives.

Outline

Some things it can do

Hey, kids, let's factor $22 - \omega$. Scratchpad

Some things it can do

Hey, kids, let's factor $22 - \omega$. Scratchpad

Let's get the rules for arithmetic in $\mathbb{Z}[\omega]$. Scratchpad

Outline

Learning transforms lives.

Widening Access

- Models like this must have been in the heads of mathematicians long before CAS.

Widening Access

- Models like this must have been in the heads of mathematicians long before CAS.
- Building them in an extensible computational environment makes this imagery more accessible.

WIDENING ACCESS

- Models like this must have been in the heads of mathematicians long before CAS.
- Building them in an extensible computational environment makes this imagery more accessible.
- Maybe, with enough experience, more people will be able to do this unplugged.

THANKS

Al Cuoco

email: acuoco@edc.org

website: http://cmeproject.edc.org/