ALGEBRA IN THE AGE OF CAS

IDEAS FROM THE CME PROJECT AND BEYOND

Al Cuoco
Center for Mathematics Education (CME), EDC

Sapienza, Università di Roma, March 5, 2009

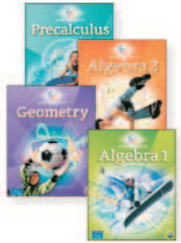
Slides available at
`www.edc.org/cmeproject`

Outline

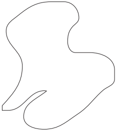
1. Some Background
   - What is *The CME Project*?
   - The *Habits of Mind* Approach
   - Some Algebraic Habits of Mind
2. Our uses of CAS
   - Three Organizing Principles
3. Examples: A case study of $x^n - 1$
   - Experimenting: Finding factors of $x^n - 1$
   - Reducing overhead: The Polynomial Factor Game
   - Modeling: Roots of Unity
4. Some Limitations to CAS
   - Cyclotomic Polynomials
5. Additional Remarks

THE CME PROJECT

- An National Science Foundation-funded 4-year curriculum
- Follows the traditional American course structure
- Uses the TI-Nspire in all 4 years
- Makes essential use of a CAS in the last two years
- Organized around mathematical habits of mind



THE *Habits of Mind* APPROACH

- The real utility of mathematics for most students comes a *style of work*, indigenous to mathematics
- Examples:
  - Is there a line that cuts the area of  in half?
  - Is the average of two averages the average of the lot?

Our use of CAS focuses on algebraic habits of mind . . .

Algebraic Habits of Mind

- Seeking regularity in repeated calculations
- “Delayed evaluation”—seeking form in calculations
- “Chunking”—changing variables in order to hide complexity
- Reasoning about and picturing calculations and operations
- Extending operations to preserve rules for calculating
- Purposefully transforming and interpreting expressions
- Seeking and specifying structural similarities

OUR USES OF CAS

- To provide students a platform for experimenting with algebraic expressions and other mathematical objects in the same way that calculators can be used to experiment with numbers.
- To make tractable and to enhance many beautiful classical topics, historically considered too technical for high school students, by reducing computational overhead.
- To allow students to build computational models of algebraic objects that have no faithful physical counterparts, highlighting similarities in algebraic structures.

EXPERIMENTING: A WEIRD FUNCTION

The number of factors over $\mathbb{Z}$ of $x^n - 1$ as a function of n.

n	number of factors of $x^n - 1$
1	
2	
3	
4	
5	
6	
7	
8	
9	

EXPERIMENTING: A WEIRD FUNCTION

The number of factors over $\mathbb{Z}$ of $x^n - 1$ as a function of n.

n	number of factors of $x^n - 1$
1	1
2	2
3	2
4	
5	
6	
7	
8	
9	

EXPERIMENTING: A WEIRD FUNCTION

The number of factors over $\mathbb{Z}$ of $x^n - 1$ as a function of n.

n	number of factors of $x^n - 1$
1	1
2	2
3	2
4	3
5	?
6	
7	
8	
9	

Scratchpad

Experimenting: A weird function

The number of factors over $\mathbb{Z}$ of $x^n - 1$ as a function of n.

n	number of factors of $x^n - 1$
1	1
2	2
3	2
4	3
5	2
6	4
7	?
8	?
9	?

Scratchpad

EXPERIMENTING: A WEIRD FUNCTION

The number of factors over $\mathbb{Z}$ of $x^n - 1$ as a function of n.

n	number of factors of $x^n - 1$
1	1
2	2
3	2
4	2
5	2
6	4
7	2
8	4
9	3

Conjectures? . . .

Experimenting: A weird function

Things that have come up in class:

- There are always at least two factors:

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)$$

- If n is odd, there are exactly two factors (but look at $n = 9$)
- OK . . . if n is prime, there are exactly two factors
- If $n = p^2$, there are three factors (ex: $x^9 - 1$)
- If $n = pq$, there are four factors (ex: $x^{15} - 1$)

$$\vdots$$

- A general conjecture gradually emerges

Scratchpad

Reducing overhead:
The Polynomial Factor Game

The *Connected Math Project* (grades 6–8) version:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30

Reducing overhead:
The Polynomial Factor Game

The CME version:

$x - 1$	$x^2 - 1$	$x^3 - 1$	$x^4 - 1$	$x^5 - 1$
$x^6 - 1$	$x^7 - 1$	$x^8 - 1$	$x^9 - 1$	$x^{10} - 1$
$x^{11} - 1$	$x^{12} - 1$	$x^{13} - 1$	$x^{14} - 1$	$x^{15} - 1$
$x^{16} - 1$	$x^{17} - 1$	$x^{18} - 1$	$x^{19} - 1$	$x^{20} - 1$
$x^{21} - 1$	$x^{22} - 1$	$x^{23} - 1$	$x^{24} - 1$	$x^{25} - 1$
$x^{26} - 1$	$x^{27} - 1$	$x^{28} - 1$	$x^{29} - 1$	$x^{30} - 1$

Scratchpad

Reducing overhead:
The Polynomial Factor Game

- “It’s the same as the middle school factor game.”
- if m is a factor of n, $x^m - 1$ is a factor of $x^n - 1$

$$\begin{aligned} x^{12} - 1 &= \left(x^3\right)^4 - 1 \\ &= (\clubsuit)^4 - 1 \\ &= (\clubsuit - 1)\left(\clubsuit^3 + \clubsuit^2 + \clubsuit + 1\right) \\ &= \left(x^3 - 1\right)\left((x^3)^3 + (x^3)^2 + (x^3) + 1\right) \\ &= \left(x^3 - 1\right)\left(x^9 + x^6 + x^3 + 1\right) \end{aligned}$$

REDUCING OVERHEAD:
THE POLYNOMIAL FACTOR GAME

- If $x^m - 1$ is a factor of $x^n - 1$, m is a factor of n

  This is harder. One way to see this is to use some arithmetic in $\mathbb{Z}[x]$.

  Another requires some facility with De Moivre's theorem and with *roots of unity*: complex numbers that are the roots of the equation

$$x^n - 1 = 0$$

MODELING:
ROOTS OF UNITY

De Moivre's Theorem implies

- The roots of $x^n - 1 = 0$ are

$$\left\{ \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \quad \middle| \quad 0 \leq k < n \right\}$$

- If $\zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, these roots are

$$1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}$$

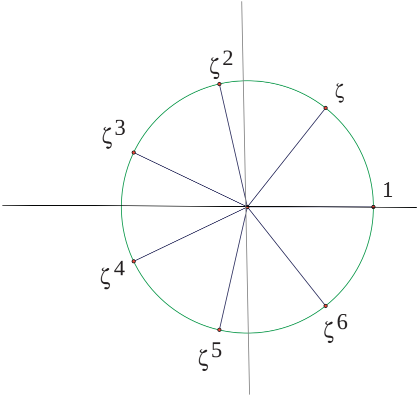
- These roots lie on the vertices of a regular n-gon of radius 1 in the complex plane

Examples

Modeling:
Roots of Unity

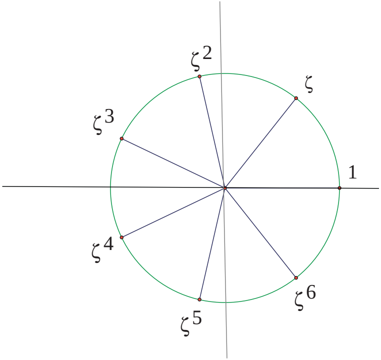
Example:

Here are the 7th roots of unity.



- The six non-real roots come in conjugate pairs.
- So $(\zeta + \zeta^6)$, $(\zeta^2 + \zeta^5)$, and $(\zeta^3 + \zeta^4)$ are real numbers.
- What cubic equation over $\mathbb{R}$ has these three numbers as roots?

MODELING:
ROOTS OF UNITY



Let

$$\alpha = \zeta + \zeta^6$$
$$\beta = \zeta^2 + \zeta^5$$
$$\gamma = \zeta^3 + \zeta^4$$

To find an equation satisfied by α, β, and γ, we need to find

- $\alpha + \beta + \gamma$
- $\alpha\beta + \alpha\gamma + \beta\gamma$
- $\alpha\beta\gamma$

One at a time...

MODELING:

ROOTS OF UNITY

The Sum:

Since $\alpha = \zeta + \zeta^6$, $\beta = \zeta^2 + \zeta^5$, and $\gamma = \zeta^3 + \zeta^4$, we have

$$\alpha + \beta + \gamma = \zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta$$

But

$$x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

So,

$$\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta = -1$$

Modeling:

Roots of Unity

The Product:

$$\alpha\beta\gamma = \left(\zeta + \zeta^6\right)\left(\zeta^2 + \zeta^5\right)\left(\zeta^3 + \zeta^4\right)$$

We can get the form of the expansion by expanding

$$\left(x + x^6\right)\left(x^2 + x^5\right)\left(x^3 + x^4\right)$$

Scratchpad

MODELING:
ROOTS OF UNITY

So,

$$\left(x+x^6\right)\left(x^2+x^5\right)\left(x^3+x^4\right) =$$

$$x^{15}+x^{14}+x^{12}+x^{11}+x^{10}+x^9+x^7+x^6$$

But if we replace x by ζ, we can replace x^7 by 1...
So, if the above expression is written as

$$(x^7-1)q(x)+r(x)$$

then replacing x by ζ will produce $r(\zeta)$, the value of $\alpha\beta\gamma$

Scratchpad

So $\alpha\beta\gamma = 1$

MODELING:
ROOTS OF UNITY

What about the “beast”? Well, $\alpha\beta + \alpha\gamma + \beta\gamma =$

$$\left(\zeta + \zeta^6\right)\left(\zeta^2 + \zeta^5\right) + \\ \left(\zeta + \zeta^6\right)\left(\zeta^3 + \zeta^4\right) + \\ \left(\zeta^2 + \zeta^5\right)\left(\zeta^3 + \zeta^4\right)$$

Scratchpad

So $\alpha\beta + \alpha\gamma + \beta\gamma = -2$ and our cubic is

$$x^3 + x^2 - 2x - 1 = 0$$

Modeling:

Roots of Unity

- In this informal way, students preview the idea that one can model $\mathbb{Q}(\zeta)$ by "remainder arithmetic" in $\mathbb{Q}(x)$, using $x^7 - 1$ as a divisor.
- In fact, one can use any divisor that has ζ as a zero—the one of smallest degree is

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

- This previews Kronecker's construction of splitting fields for algebraic equations.

Back to the factors of $x^n - 1$

Leaving the CME Project for now

A closer look at the factors:

1	$-1+x$
2	$(-1+x)\,(1+x)$
3	$(-1+x)\,\left(1+x+x^2\right)$
4	$(-1+x)\,(1+x)\,\left(1+x^2\right)$
5	$(-1+x)\,\left(1+x+x^2+x^3+x^4\right)$
6	$(-1+x)\,(1+x)\,\left(1-x+x^2\right)\,\left(1+x+x^2\right)$
7	$(-1+x)\,\left(1+x+x^2+x^3+x^4+x^5+x^6\right)$
8	$(-1+x)\,(1+x)\,\left(1+x^2\right)\,\left(1+x^4\right)$
9	$(-1+x)\,\left(1+x+x^2\right)\,\left(1+x^3+x^6\right)$
10	$(-1+x)\,(1+x)\,\left(1-x+x^2-x^3+x^4\right)\,\left(1+x+x^2+x^3+x^4\right)$

Scratchpad

A closer look at the factors

The degrees of the factors:

1	1
2	1, 1
3	1, 2
4	1, 1, 2
5	1, 4
6	1, 1, 2, 2
7	1, 6
8	1, 1, 2, 4
9	1, 2, 6
10	1, 1, 4, 4
11	1, 10
12	1, 1, 2, 2, 2, 4
13	1, 12
14	1, 1, 6, 6
15	1, 2, 4, 8
16	1, 1, 2, 4, 8
17	1, 16
18	1, 1, 2, 2, 6, 6
19	1, 18
20	1, 1, 2, 4, 4, 8

Scratchpad

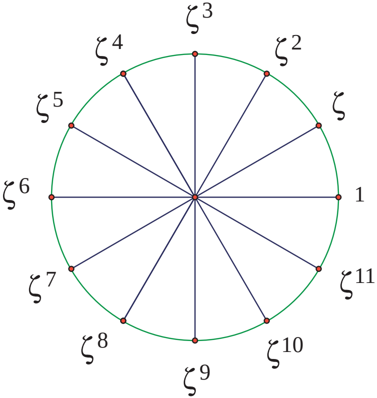
A CLOSER LOOK AT THE FACTORS

Questions, Conjectures, Ideas. . .

- Are the coefficients of the factors always ±1 or 0?
  - No. . . consider $n = 105$. Scratchpad
- Is 105 a freak of nature?
  - No. We need a little more machinery to see the landscape.
- What's up with the degrees?
  - How do the degrees of the factors of $x^n - 1$ partition n?

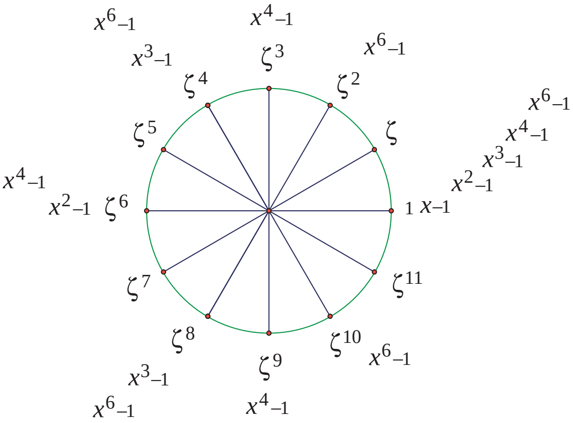
Cyclotomic polynomials

Here are the 12th roots of unity:



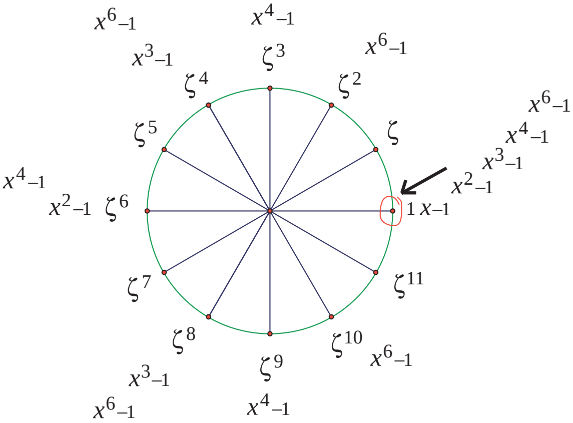
Cyclotomic polynomials

Some are roots of $x^n - 1 = 0$ for $n < 12$:



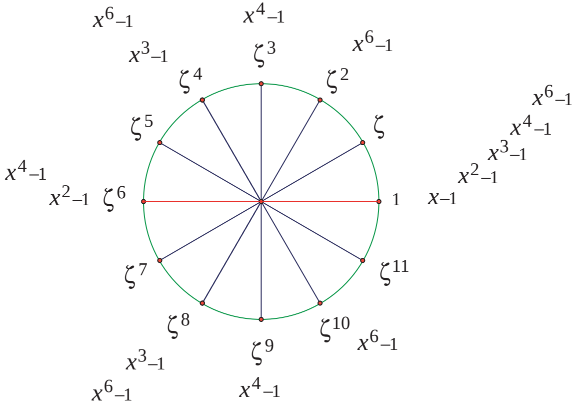
Cyclotomic polynomials

Some are “first” roots of unity:



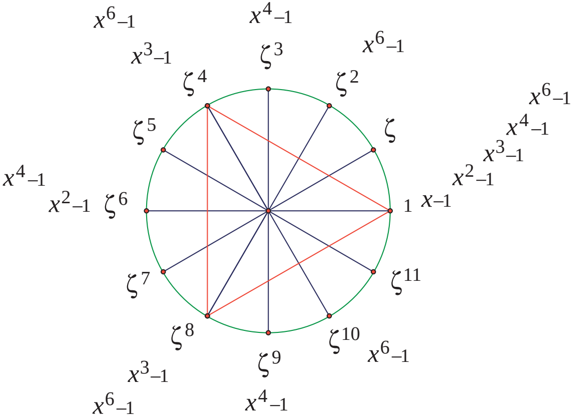
Cyclotomic polynomials

Some are "square" roots of unity:



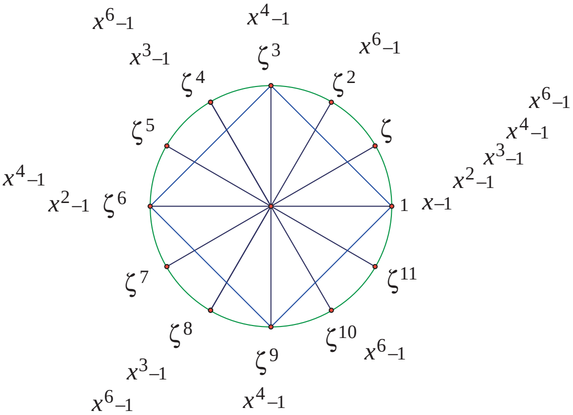
Cyclotomic polynomials

Some are cube roots of unity:



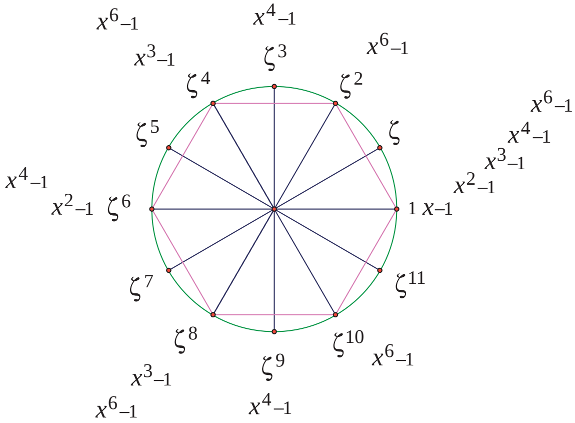
Cyclotomic polynomials

Some are fourth roots of unity:



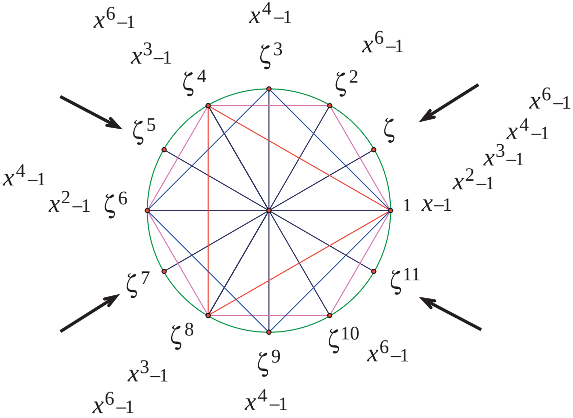
CYCLOTOMIC POLYNOMIALS

And some are sixth roots of unity:



Cyclotomic polynomials

Left are the *primitive* 12th roots of unity: ζ, ζ^5, ζ^7, and ζ^{11}.



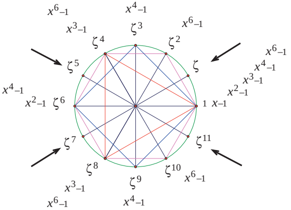
Scratchpad

Cyclotomic polynomials

So, the roots of $x^{12} - 1 = 0$ break up like this

$$\begin{array}{cccccc}
(x-1) & (x+1) & (x^2+x+1) & (x^2+1) & (x^2-x+1) & (x^4-x^2+1) \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
1 & -1 & -\frac{1}{2} \pm i\frac{\sqrt{3}}{2} & \pm i & \frac{1}{2} \pm i\frac{\sqrt{3}}{2} & \pm\frac{\sqrt{3}}{2} \pm \frac{1}{2}i \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
\zeta^0 & \zeta^6 & \{\zeta^4, \zeta^8\} & \{\zeta^3, \zeta^9\} & \{\zeta^2, \zeta^{10}\} & \{\zeta, \zeta^5, \zeta^7, \zeta^{11}\} \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
\text{first} & \text{second} & \text{third} & \text{fourth} & \text{sixth} & \text{twelvth}
\end{array}$$

- There is one factor for every divisor d of 12.
- The zeros of the factor for d are the primitive dth roots of 1.
- The primitive 12th roots are ζ^k where $\gcd(k, 12) = 1$



Cyclotomic polynomials

In general

- If $\zeta_m = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$, the primitive *m*th roots of unity are

$$\left\{\zeta_m^k \mid \gcd(k,m) = 1\right\}$$

- If

$$\psi_m(x) = \prod_{\substack{1 \le k \le m \\ \gcd(k,m)=1}} \left(x - \zeta_m^k\right)$$

  then

  - $\psi_m(x)$ has integer coefficients and is irreducible over $\mathbb{Z}$,
  - the degree of $\psi_m(x)$ is $\phi(m)$ (Euler's ϕ-function), and. . .

Cyclotomic polynomials

The CAS factorization of $x^n - 1$ is precisely

$$x^n - 1 = \prod_{d \mid n} \psi_d(x)$$

So, for example, $x^{12} - 1 =$

$$\begin{tikzcd}
(x-1) & (x+1) & (x^2+x+1) & (x^2+1) & (x^2-x+1) & (x^4-x^2+1) \\
\psi_1(x) \arrow[u] & \psi_2(x) \arrow[u] & \psi_3(x) \arrow[u] & \psi_4(x) \arrow[u] & \psi_6(x) \arrow[u] & \psi_{12}(x) \arrow[u] \\
\phi(1)=1 \arrow[u] & \phi(2)=1 \arrow[u] & \phi(3)=2 \arrow[u] & \phi(4)=2 \arrow[u] & \phi(6)=2 \arrow[u] & \phi(12)=4 \arrow[u]
\end{tikzcd}$$

Cyclotomic polynomials

Consequences:

- The partition of n given by the degrees of factors is Scratchpad

$$\{\phi(d) \mid d \text{ is a factor of } n\}$$

- As a bonus, we get the famous

$$\sum_{d|n} \phi(d) = n$$

- We can compute the irreducible factors recursively from $x^n - 1 = \prod_{d \mid n} \psi_d(x)$: Scratchpad

$$\psi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d \mid n \\ d<n}} \psi_d(x)}$$

Cyclotomic polynomials

A seemingly wonderful theorem:

If k is odd, and if $p_1 < p_2 < \cdots < p_k$ is a "front-loaded" sequence of primes—the sum of the first two in the sequence is greater than the last—and if n is the product of all the primes in the sequence, then $\psi_n(x)$ has $-k+1$ and $-k+2$ as coefficients.

Example: since $105 = 3 \cdot 5 \cdot 7$, and $\{3, 5, 7\}$ is a front-loaded sequence of length 3, $\psi_{105}(x)$ has a coefficient of -2. In fact, it's the coefficient of x^7. Scratchpad

More details in "On Coefficients of Cyclotomic Polynomials." Jiro Suzuki: Proc. Japan Acad., Ser. A,1987.

NB: $\exists$ a front-loaded sequence of length k for every odd $k \geq 3$.

Cyclotomic polynomials

To get a coefficient of -3, the theorem demands that we look at ψ_n where $n = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 1062347$.

(A much smaller value of n works as well.)

This is where the trouble started.

Neither Nspire nor Mathematica could calculate $\psi_{1062347}(x)$.

So, I contacted Cleve Moler, creator of MATLAB.

Cyclotomic polynomials

Hi Cleve,

It's known that coefficients of cyclotomic polynomials can be made as large as you like.

One way is to take the *n*th polynomial where n is a product of k distinct primes (k odd) so that the sum of the first two is larger than the last. The first of these is $k = 105 = 3 \cdot 5 \cdot 7$.

The first length 5 sequence is $n = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$, but neither the Nspire nor Mathematica will generate the polynomial (or its coefficient list).

Can MATLAB do it?

Al

Cyclotomic polynomials

By itself, MATLAB cannot handle integers larger than 2^{52}. With the Symbolic Toolbox, MATLAB can handle arbitrarily large integers. Without Mathematica's function, how would you generate $\psi_n(x)$?

—Cleve

Cyclotomic polynomials

Well, Mathematica has a built in “Cyclotomic” command, so I typed

```
Cyclotomic[11*13*17*19*23, x]
```

It just stalls. On the Nspire, I used the fact that if $\psi_n(x)$ is the nth cyclotomic poly, then

$$\psi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d \mid n \\ d<n}} \psi_d(x)}$$

There’s also a recurrence that uses the Möebius function. Or,

$$\prod (x - e^{\frac{2k\pi i}{n}})$$

Where k ranges over the integers relatively prime to n

—Al

Cyclotomic Polynomials

Attached are two programs. I think “cyclo” is what we want, but it never finishes. “cyclo2” is a simplified version. It doesn’t finish either.

I’m actually testing the next version of the Symbolic Toolbox. We haven’t released it yet. I’m checking with the guys working on this next version, and I’m going to let “cyclo” run for awhile—maybe overnight.

It’s an important point—talking to a live mathematician is very different from talking to a CAS.

I have another idea to try—more later. . .

—Cleve

Cyclotomic polynomials

The next day

$\vdots$

Cyclotomic polynomials

Al—

For $n = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 1062347$, the degree of $\psi_n(x)$ is 760320. The coefficients range from -1749 to $+1694$. There are 11804 zero coefficients. The average coefficient magnitude is 409.9.

My MATLAB program is attached. It uses the Symbolic Toolbox for the number theoretic functions moebius(n) and divisors(n), but *not* for any polynomial manipulations.

Polynomials are represented as MATLAB vectors with integer elements. Polynomial multiplication and division is done by MATLAB vector convolution and deconvolution.

$\vdots$

CYCLOTOMIC POLYNOMIALS

$\psi_n(x)$ is computed from the ratio of two polynomials, a numerator of degree 1105920 and a denominator of degree 345600. It takes about 6 minutes on my laptop to compute the numerator and denominator and then about $2\frac{1}{2}$ hours to compute their ratio using only the deconvolution.

I've saved the results. Anything else you'd like to know?

—Cleve

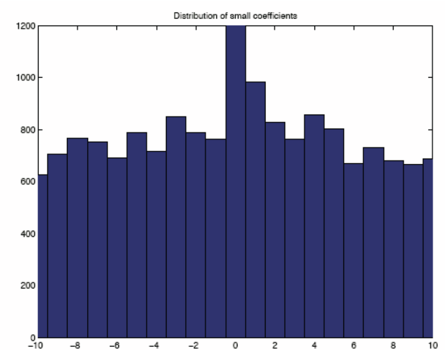
$$\psi_n(x) = \prod_{d|n} \left(1 - x^{\frac{n}{d}}\right)^{\mu(d)}$$

Cyclotomic Polynomials

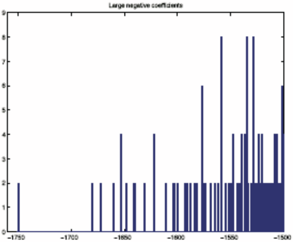
```
length(find(p==4))
ans=856
length(find(p==-4))
ans=716
```

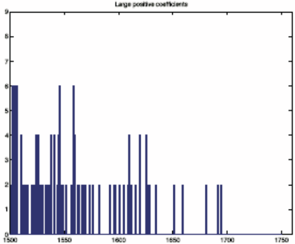
You might find the attached histograms interesting.

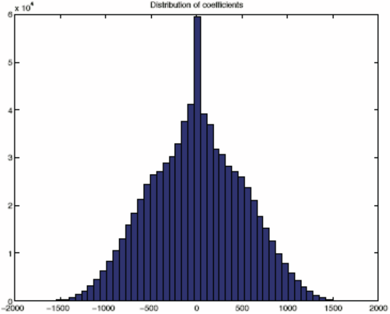
—Cleve



Cyclotomic Polynomials







In Summary: A Computational Perspective

- …talking to a live mathematician is very different from talking to a CAS.
- It's important to point out that I did the heavy lifting without using a CAS .
- By the way, the convolutions and, especially, the deconvolution can be done in a few minutes instead of a few hours using FFTs, but roundoff errors get in the way. For $n = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$, the computed results are contaminated enough that rounding them to integers produces some coefficients that are off by ± 1.

—Cleve

In Summary: A Mathematical Perspective

- Mathematical objects are *real*.
  - Mathematical phenomena exhibit all of the intricate and textured features present in physical phenomena.
- Mathematical thinking is a wonderful thing.

  The human mind can establish facts about mathematical objects even when the objects are difficult (or impossible) to write down explicitly.

USING A CAS IN HIGH SCHOOL: OTHER EXAMPLES

The CME Project uses a CAS to

1. Experiment with algebra: Chebyshev polynomials
2. Reduce computational overhead: Lagrange interpolation and Newton's Difference Formula
3. Use polynomials as modeling tools: Generating functions

Just for Fun

Newton's Difference Formula

Input	Output	Δ	Δ^2	Δ^3
0	1	-2	14	12
1	-1	12	26	12
2	11	38	38	12
3	49	76	50	12
4	125	126	62	12
5	251	188	74	
6	439	262		
7	701			

Scratchpad

GRAZIE MOLTO

Al Cuoco

Center for Mathematics Education

Education Development Center

acuoco@edc.org