Finding Minimal Polynomials with a Norm Calculator

Eric Errthum
Winona State University
eerrthum@winona.edu

October 18, 2008

Algebraic Review

- An algebraic number, ζ, is a root of an irreducible monic polynomial with rational coefficients.

Algebraic Review

- An algebraic number, ζ, is a root of an irreducible monic polynomial with rational coefficients.

Examples

$$\zeta = i \quad \Rightarrow \quad x^2 + 1 = 0$$

$$\zeta = \frac{4}{\sqrt{\sqrt[3]{9} + 7\sqrt[3]{3}}} \quad \Rightarrow \quad x^6 + \frac{504}{519}x^4 - \frac{2048}{519}$$

Algebraic Review

- An algebraic number, ζ, is a root of an irreducible monic polynomial with rational coefficients.

Examples

$$\zeta = i \quad \Rightarrow \quad x^2 + 1 = 0$$

$$\zeta = \frac{4}{\sqrt{\sqrt[3]{9} + 7\sqrt[3]{3}}} \quad \Rightarrow \quad x^6 + \frac{504}{519}x^4 - \frac{2048}{519}$$

- This polynomial, $M_\zeta(x)$, is called the minimal polynomial and

$$M_\zeta(x) = \prod_i (x - \sigma_i(\zeta))$$

where $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Algebraic Review

- An algebraic number, ζ, is a root of an irreducible monic polynomial with rational coefficients.

Examples

$$\zeta = i \quad \Rightarrow \quad x^2 + 1 = 0$$
$$\zeta = \frac{4}{\sqrt{\sqrt[3]{9} + 7\sqrt[3]{3}}} \quad \Rightarrow \quad x^6 + \frac{504}{519}x^4 - \frac{2048}{519}$$

- This polynomial, $M_\zeta(x)$, is called the minimal polynomial and

$$M_\zeta(x) = \prod_i (x - \sigma_i(\zeta))$$

where $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

- The (absolute) norm of ζ, $\mathrm{norm}(\zeta) = |\prod \sigma_i(\zeta)|$, is the absolute value of the constant term of $M_\zeta(x)$.

Problem Statement

Given

- A collection of unknown algbraic numbers $\{\zeta_1, \zeta_2, \dots\}$ whose minimal polynomials have known degrees $\{d_1, d_2, \dots\}$.

Problem Statement

Given

- A collection of unknown algbraic numbers $\{\zeta_1, \zeta_2, \ldots\}$ whose minimal polynomials have known degrees $\{d_1, d_2, \ldots\}$.
- An algorithm that can compute the norm of an unknown algebraic number (norm calculator).

Problem Statement

Given

- A collection of unknown algbraic numbers $\{\zeta_1, \zeta_2, \ldots\}$ whose minimal polynomials have known degrees $\{d_1, d_2, \ldots\}$.
- An algorithm that can compute the norm of an unknown algebraic number (norm calculator).

Find

- The minimal polynomials for (at least some of) the ζ_k's?

Shimura Curves

- The Shimura curve S_6 is a Riemannian surface of genus zero.

Shimura Curves

- The Shimura curve S_6 is a Riemannian surface of genus zero.
- An isomorphism $J : S_6 \xrightarrow{\sim} \mathbb{P}^1$ exists.

Shimura Curves

- The Shimura curve S_6 is a Riemannian surface of genus zero.
- An isomorphism $J : S_6 \xrightarrow{\sim} \mathbb{P}^1$ exists.
- It can be uniquely specified by choosing the three points that map to 0, 1, and ∞.

Shimura Curves

- The Shimura curve S_6 is a Riemannian surface of genus zero.
- An isomorphism $J : S_6 \xrightarrow{\sim} \mathbb{P}^1$ exists.
- It can be uniquely specified by choosing the three points that map to 0, 1, and ∞.
- Due to the properties of Shimura curves, no formula exists for such a map.

CM Points on the Shimura Curve

- There is a collection of "special" points $\{s_k\} \subset S_6$ called complex multiplication (CM) points.

CM Points on the Shimura Curve

- There is a collection of "special" points $\{s_k\} \subset S_6$ called complex multiplication (CM) points.
- Three of these, s_3, s_4, and s_{24}, are *really* special, so specify J by

$$(s_3, s_4, s_{24}) \xrightarrow{J} (0, 1, \infty).$$

CM Points on the Shimura Curve

- There is a collection of "special" points $\{s_k\} \subset S_6$ called complex multiplication (CM) points.
- Three of these, s_3, s_4, and s_{24}, are *really* special, so specify J by

$$(s_3, s_4, s_{24}) \xrightarrow{J} (0, 1, \infty).$$

- Then J maps all CM points to algebraic numbers.

CM Points on the Shimura Curve

- There is a collection of "special" points $\{s_k\} \subset S_6$ called complex multiplication (CM) points.
- Three of these, s_3, s_4, and s_{24}, are *really* special, so specify J by

$$(s_3, s_4, s_{24}) \xrightarrow{J} (0, 1, \infty).$$

- Then J maps all CM points to algebraic numbers.
- There exists an algorithm that calculates norm$(J(s_k))$ for s_k a CM point. (Errthum, 2007)

CM Points on the Shimura Curve

- There is a collection of "special" points $\{s_k\} \subset S_6$ called complex multiplication (CM) points.
- Three of these, s_3, s_4, and s_{24}, are *really* special, so specify J by

$$(s_3, s_4, s_{24}) \xrightarrow{J} (0, 1, \infty).$$

- Then J maps all CM points to algebraic numbers.
- There exists an algorithm that calculates norm$(J(s_k))$ for s_k a CM point. (Errthum, 2007)
- Using genus theory of groups, we can calculate d_k, the degree of $M_{J(s_k)}(x)$.

CM Points on the Shimura Curve

- There is a collection of "special" points $\{s_k\} \subset S_6$ called complex multiplication (CM) points.
- Three of these, s_3, s_4, and s_{24}, are *really* special, so specify J by

$$(s_3, s_4, s_{24}) \xrightarrow{J} (0, 1, \infty).$$

- Then J maps all CM points to algebraic numbers.
- There exists an algorithm that calculates norm$(J(s_k))$ for s_k a CM point. (Errthum, 2007)
- Using genus theory of groups, we can calculate d_k, the degree of $M_{J(s_k)}(x)$.

Back to the problem: Let $\{\zeta_k\} = \{J(s_k)\}$.

First Trick

- For a finite number of indices r, $M_{J(s_r)}(x)$ has degree 1, i.e. ζ_r is a rational number.

First Trick

- For a finite number of indices r, $M_{J(s_r)}(x)$ has degree 1, i.e. ζ_r is a rational number.
- $$\mathrm{norm}(\zeta_r) = \pm\zeta_r.$$

First Trick

- For a finite number of indices r, $M_{J(s_r)}(x)$ has degree 1, i.e. ζ_r is a rational number.
- $$\mathrm{norm}(\zeta_r) = \pm\zeta_r.$$
- Use a new J_1 by taking $(s_3, s_4, s_{24}) \to (1, 0, \infty)$ instead of $(0, 1, \infty)$.
$$J_1(s) = 1 - J(s).$$

First Trick

- For a finite number of indices r, $M_{J(s_r)}(x)$ has degree 1, i.e. ζ_r is a rational number.
- $$\text{norm}(\zeta_r) = \pm\zeta_r.$$
- Use a new J_1 by taking $(s_3, s_4, s_{24}) \to (1, 0, \infty)$ instead of $(0, 1, \infty)$.
$$J_1(s) = 1 - J(s).$$

Example

$$\text{norm}(J(s_r)) = 4/5 \text{ and } \text{norm}(1 - J(s_r)) = 9/5$$
$$\Rightarrow \zeta_r = J(s_r) = -4/5$$

First Trick

- For a finite number of indices r, $M_{J(s_r)}(x)$ has degree 1, i.e. ζ_r is a rational number.
- $$\text{norm}(\zeta_r) = \pm\zeta_r.$$
- Use a new J_1 by taking $(s_3, s_4, s_{24}) \to (1, 0, \infty)$ instead of $(0, 1, \infty)$.
$$J_1(s) = 1 - J(s).$$

Example

$$\text{norm}(J(s_r)) = 4/5 \text{ and } \text{norm}(1 - J(s_r)) = 9/5$$
$$\Rightarrow \zeta_r = J(s_r) = -4/5$$

- Can calculate all rational ζ_r this way.

Second Trick

- Choose ζ_k with d_k small.

Second Trick

- Choose ζ_k with d_k small.
- For $d_k + 1$ choices of r, specify $J_r(s) = \zeta_r - J(s)$ by

$$(s_3, s_r, s_{24}) \xrightarrow{J_r} (\zeta_r, 0, \infty).$$

Second Trick

- Choose ζ_k with d_k small.
- For $d_k + 1$ choices of r, specify $J_r(s) = \zeta_r - J(s)$ by

$$(s_3, s_r, s_{24}) \xrightarrow{J_r} (\zeta_r, 0, \infty).$$

- $$\mathrm{norm}(\zeta_r - J(s_k)) \quad = \quad \left|\prod_i \sigma_i(\zeta_r - J(s_k))\right|$$

Second Trick

- Choose ζ_k with d_k small.
- For $d_k + 1$ choices of r, specify $J_r(s) = \zeta_r - J(s)$ by

$$(s_3, s_r, s_{24}) \xrightarrow{J_r} (\zeta_r, 0, \infty).$$

- $$\begin{aligned} \operatorname{norm}(\zeta_r - J(s_k)) &= \left| \prod_i \sigma_i(\zeta_r - J(s_k)) \right| \\ &= \left| \prod_i \sigma_i(\zeta_r - \zeta_k) \right| \end{aligned}$$

Second Trick

- Choose ζ_k with d_k small.
- For $d_k + 1$ choices of r, specify $J_r(s) = \zeta_r - J(s)$ by

$$(s_3, s_r, s_{24}) \xrightarrow{J_r} (\zeta_r, 0, \infty).$$

- $$\begin{aligned} \mathrm{norm}(\zeta_r - J(s_k)) &= \left| \prod_i \sigma_i(\zeta_r - J(s_k)) \right| \\ &= \left| \prod_i \sigma_i(\zeta_r - \zeta_k) \right| \\ &= \left| \prod_i (\zeta_r - \sigma_i(\zeta_k)) \right| \end{aligned}$$

Second Trick

- Choose ζ_k with d_k small.
- For $d_k + 1$ choices of r, specify $J_r(s) = \zeta_r - J(s)$ by
$$(s_3, s_r, s_{24}) \xrightarrow{J_r} (\zeta_r, 0, \infty).$$
- $$\begin{aligned} \mathrm{norm}(\zeta_r - J(s_k)) &= \left|\prod_i \sigma_i(\zeta_r - J(s_k))\right| \\ &= \left|\prod_i \sigma_i(\zeta_r - \zeta_k)\right| \\ &= \left|\prod_i (\zeta_r - \sigma_i(\zeta_k))\right| \\ &= |M_{\zeta_k}(\zeta_r)| \end{aligned}$$

Brute Force

- So we know $d_k + 1$ points on the curve $y = |M_{\zeta_k}(x)|$.

Brute Force

- So we know $d_k + 1$ points on the curve $y = |M_{\zeta_k}(x)|$.
- If it wasn't for the absolute value, we could use a standard polynomial fit and be done.

Brute Force

- So we know $d_k + 1$ points on the curve $y = |M_{\zeta_k}(x)|$.
- If it wasn't for the absolute value, we could use a standard polynomial fit and be done.
- Go through the 2^{d_k} combinations of minus signs on the values until you find a monic polynomial.
  (There's only ever one. Proof?)

Brute Force

- So we know $d_k + 1$ points on the curve $y = |M_{\zeta_k}(x)|$.
- If it wasn't for the absolute value, we could use a standard polynomial fit and be done.
- Go through the 2^{d_k} combinations of minus signs on the values until you find a monic polynomial.
  (There's only ever one. Proof?)
- If there are R rational ζ_r, then we can use this method to find the minimal polynomial of any ζ_k with $d_k \leq R - 2$.

Example

- $\text{norm}(\zeta) = \frac{10}{17}$ and $d = 3$.

Example

- $\text{norm}(\zeta) = \frac{10}{17}$ and $d = 3$.
- We use the four CM points that map to 0, 1, $\frac{-4}{5}$, and $\frac{2}{3}$ to find the data points:

Example

- $\text{norm}(\zeta) = \frac{10}{17}$ and $d = 3$.
- We use the four CM points that map to 0, 1, $\frac{-4}{5}$, and $\frac{2}{3}$ to find the data points:

$$(0, \text{norm}(\zeta)) = \left(0, \frac{10}{17}\right)$$

$$(1, \text{norm}\left(1 - \zeta\right)) = \left(1, \frac{25}{102}\right)$$

$$\left(\frac{-4}{5}, \text{norm}\left(\frac{-4}{5} - \zeta\right)\right) = \left(\frac{-4}{5}, \frac{5246}{6375}\right)$$

$$\left(\frac{2}{3}, \text{norm}\left(\frac{2}{3} - \zeta\right)\right) = \left(\frac{2}{3}, \frac{104}{459}\right)$$

Example

- $\text{norm}(\zeta) = \frac{10}{17}$ and $d = 3$.
- We use the four CM points that map to 0, 1, $\frac{-4}{5}$, and $\frac{2}{3}$ to find the data points:

$$(0, \text{norm}(\zeta)) = \left(0, \frac{10}{17}\right)$$
$$(1, \text{norm}\,(1-\zeta)) = \left(1, \frac{25}{102}\right)$$
$$\left(\frac{-4}{5}, \text{norm}\left(\frac{-4}{5}-\zeta\right)\right) = \left(\frac{-4}{5}, \frac{5246}{6375}\right)$$
$$\left(\frac{2}{3}, \text{norm}\left(\frac{2}{3}-\zeta\right)\right) = \left(\frac{2}{3}, \frac{104}{459}\right)$$

- Possible minimal polynomials:

$$\begin{aligned}
y &= \frac{10}{17} - \frac{3316}{5049}x - \frac{1141}{10098}x^2 + \frac{718}{1683}x^3 \\
y &= \frac{10}{17} - \frac{124}{561}x - \frac{83}{374}x^2 - \frac{73}{187}x^3 \\
y &= \frac{10}{17} - \frac{812}{459}x - \frac{359}{918}x^2 + \frac{278}{153}x^3 \\
y &= \frac{10}{17} - \frac{4}{3}x - \frac{1}{2}x^2 + x^3 \\
y &= \frac{10}{17} - \frac{7}{51}x - \frac{24}{17}x^2 + \frac{41}{34}x^3 \\
y &= \frac{10}{17} + \frac{137}{459}x - \frac{698}{459}x^2 + \frac{7}{18}x^3 \\
y &= \frac{10}{17} - \frac{701}{561}x - \frac{316}{187}x^2 + \frac{971}{374}x^3 \\
y &= \frac{10}{17} - \frac{4109}{5049}x - \frac{9082}{5049}x^2 + \frac{5989}{3366}x^3
\end{aligned}$$

Example

- $\text{norm}(\zeta) = \frac{10}{17}$ and $d = 3$.
- We use the four CM points that map to 0, 1, $\frac{-4}{5}$, and $\frac{2}{3}$ to find the data points:

$$(0, \text{norm}(\zeta)) = (0, \tfrac{10}{17})$$

$$(1, \text{norm}\,(1-\zeta)) = (1, \tfrac{25}{102})$$

$$\left(\tfrac{-4}{5}, \text{norm}\,\left(\tfrac{-4}{5}-\zeta\right)\right) = \left(\tfrac{-4}{5}, \tfrac{5246}{6375}\right)$$

$$\left(\tfrac{2}{3}, \text{norm}\,\left(\tfrac{2}{3}-\zeta\right)\right) = \left(\tfrac{2}{3}, \tfrac{104}{459}\right)$$

- Possible minimal polynomials:

$$\begin{aligned}
y &= \frac{10}{17} - \frac{3316}{5049}x - \frac{1141}{10098}x^2 + \frac{718}{1683}x^3 \\
y &= \frac{10}{17} - \frac{124}{561}x - \frac{83}{374}x^2 - \frac{73}{187}x^3 \\
y &= \frac{10}{17} - \frac{812}{459}x - \frac{359}{918}x^2 + \frac{278}{153}x^3 \\
y &= \frac{10}{17} - \frac{4}{3}x - \frac{1}{2}x^2 + x^3 \\
y &= \frac{10}{17} - \frac{7}{51}x - \frac{24}{17}x^2 + \frac{41}{34}x^3 \\
y &= \frac{10}{17} + \frac{137}{459}x - \frac{698}{459}x^2 + \frac{7}{18}x^3 \\
y &= \frac{10}{17} - \frac{701}{561}x - \frac{316}{187}x^2 + \frac{971}{374}x^3 \\
y &= \frac{10}{17} - \frac{4109}{5049}x - \frac{9082}{5049}x^2 + \frac{5989}{3366}x^3
\end{aligned}$$

So the minimal polynomial of ζ is $M_\zeta(x) = \frac{10}{17} - \frac{4}{3}x - \frac{1}{2}x^2 + x^3$.

Thanks

Questions?

eerrthum@winona.edu