Monogenic S_4 Quartic Fields Arising from Elliptic Curves

Joint work with Kate Stange and Alden Gassert

Hanson Smith

University of Colorado, Boulder

Table of contents

Background

Monogenic Fields

Let K be a number field. We say K is **monogenic** if the ring of integers $\mathcal{O}_K$ admits a power $\mathbb{Z}$-basis. That is, if there is some monic, irreducible $f(x) \in \mathbb{Z}[x]$ with a root θ such that $\mathcal{O}_K$ has a $\mathbb{Z}$-basis $\left\{1, \theta, \ldots, \theta^{n-1}\right\}$, then K is monogenic.

Monogenic Fields

Let K be a number field. We say K is **monogenic** if the ring of integers $\mathcal{O}_K$ admits a power $\mathbb{Z}$-basis. That is, if there is some monic, irreducible $f(x) \in \mathbb{Z}[x]$ with a root θ such that $\mathcal{O}_K$ has a $\mathbb{Z}$-basis $\left\{1, \theta, \ldots, \theta^{n-1}\right\}$, then K is monogenic.

Examples: Quadratic fields. The field $\mathbb{Q}(\sqrt{d})$ has a ring of integers with $\mathbb{Z}$-basis $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ if $d \equiv 1$ modulo 4 and $\left\{1, \sqrt{d}\right\}$ otherwise.

Monogenic Fields

Let K be a number field. We say K is **monogenic** if the ring of integers $\mathcal{O}_K$ admits a power $\mathbb{Z}$-basis. That is, if there is some monic, irreducible $f(x) \in \mathbb{Z}[x]$ with a root θ such that $\mathcal{O}_K$ has a $\mathbb{Z}$-basis $\left\{1, \theta, \ldots, \theta^{n-1}\right\}$, then K is monogenic.

Examples: Quadratic fields. The field $\mathbb{Q}(\sqrt{d})$ has a ring of integers with $\mathbb{Z}$-basis $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ if $d \equiv 1$ modulo 4 and $\left\{1, \sqrt{d}\right\}$ otherwise.

Cyclotomic fields. The ring of integers $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ has $\mathbb{Z}$-basis $\left\{1, \zeta_p, \ldots, \zeta_p^{p-2}\right\}$.

A Non-monogenic Field

Consider $x^3 - x^2 - 2x - 8$ and let θ be a root. Dedekind showed $\mathbb{Q}(\theta)$ is *not* monogenic.

A Non-monogenic Field

Consider $x^3 - x^2 - 2x - 8$ and let θ be a root. Dedekind showed $\mathbb{Q}(\theta)$ is *not* monogenic.

A "good" $\mathbb{Z}$ basis is

$$\left\{1, \frac{1}{2}(\theta + \theta^2), \theta^2\right\}.$$

Division Polynomials and Partial Torsion Fields

For the rest of the talk let E be an elliptic curve over $\mathbb{Q}$. If $P = (x, y) \in E(\mathbb{Q})$ then we can describe the multiplication by m map quite explicitly:

$$[m]P = \left(\frac{\phi_m(P)}{\Psi_m(P)^2}, \frac{\omega_m(P)}{\Psi_m(P)^3} \right)$$

where $\phi_m, \Psi_m, \omega_m \in \mathbb{Z}[x, y]$. If m is odd then $\Psi_m \in \mathbb{Z}[x]$.

Division Polynomials and Partial Torsion Fields

For the rest of the talk let E be an elliptic curve over $\mathbb{Q}$. If $P = (x, y) \in E(\mathbb{Q})$ then we can describe the multiplication by m map quite explicitly:

$$[m]P = \left(\frac{\phi_m(P)}{\Psi_m(P)^2}, \frac{\omega_m(P)}{\Psi_m(P)^3} \right)$$

where $\phi_m, \Psi_m, \omega_m \in \mathbb{Z}[x, y]$. If m is odd then $\Psi_m \in \mathbb{Z}[x]$.

We call Ψ_m the m^{th} **division polynomial**.

Division Polynomials and Partial Torsion Fields

For the rest of the talk let E be an elliptic curve over $\mathbb{Q}$. If $P = (x, y) \in E(\mathbb{Q})$ then we can describe the multiplication by m map quite explicitly:

$$[m]P = \left(\frac{\phi_m(P)}{\Psi_m(P)^2}, \frac{\omega_m(P)}{\Psi_m(P)^3} \right)$$

where $\phi_m, \Psi_m, \omega_m \in \mathbb{Z}[x, y]$. If m is odd then $\Psi_m \in \mathbb{Z}[x]$.

We call Ψ_m the m^{th} **division polynomial**.

Generally, $\mathbb{Q}(E[m])$ is called the m^{th} **torsion field** or m^{th} **division field**. If m is odd and Ψ_m is irreducible we define the m^{th} **partial torsion field** to be the extension of $\mathbb{Q}$ obtained by a root of Ψ_m.

Another Definition of Division Polynomials

If we write

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then we can define Ψ_n recursively starting with

$$\Psi_1 = 1,$$

$$\Psi_2 = 2y + a_1x + a_3,$$

$$\Psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$

$$\frac{\Psi_4}{\Psi_2} = 2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2),$$

and using the formulas

$$\Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3 \qquad \text{for } m \geq 2,$$

$$\Psi_{2m+1}\Psi_2 = \Psi_{m-1}^2\Psi_m\Psi_{m+2} - \Psi_{m-2}\Psi_m\Psi_{m+1}^2 \qquad \text{for } m \geq 3.$$

The Main Result and Context

A Monogenic Family

Theorem

Suppose that $\alpha \pm 8$ *are squarefree, where* $\alpha \in \mathbb{Z}$*. Let* θ *be a root of the irreducible polynomial* $T^4 - 6T^2 - \alpha T - 3$*. Then the ring of integers of* $\mathbb{Q}(\theta)$ *has* $\mathbb{Z}$*-basis* $\left\{1, \theta, \theta^2, \theta^3\right\}$*. That is,* $\mathbb{Q}(\theta)$ *is a monogenic quartic field. Moreover,* $\mathbb{Q}(\theta)$ *has Galois group* S_4*.*

Our Main Result

Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$, such that some twist E' of E has a 4-torsion point defined over $\mathbb{Q}$.

Our Main Result

Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$, such that some twist E' of E has a 4-torsion point defined over $\mathbb{Q}$. Then the following are equivalent:

1. *E' has reduction types I_1^* and I_1 only;*
2. *E has j-invariant with squarefree denominator except a possible factor of 4.*
3. *E has j-invariant $j = \frac{(\alpha^2-48)^3}{(\alpha-8)(\alpha+8)}$, where $\alpha \in \mathbb{Z}$, $\alpha \pm 8$ are squarefree.*

Our Main Result

Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$, such that some twist E' of E has a 4-torsion point defined over $\mathbb{Q}$. Then the following are equivalent:

1. *E' has reduction types I_1^* and I_1 only;*
2. *E has j-invariant with squarefree denominator except a possible factor of 4.*
3. *E has j-invariant $j = \frac{(\alpha^2-48)^3}{(\alpha-8)(\alpha+8)}$, where $\alpha \in \mathbb{Z}$, $\alpha \pm 8$ are squarefree.*

Let θ be a root of Ψ_3. If any of the above hypotheses holds, then the third partial torsion field, $\mathbb{Q}(\theta)$, is monogenic with a generator given by a root of $T^4 - 6T^2 - \alpha T - 3$.

Our Main Result

Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$, such that some twist E' of E has a 4-torsion point defined over $\mathbb{Q}$. Then the following are equivalent:

1. *E' has reduction types I_1^* and I_1 only;*
2. *E has j-invariant with squarefree denominator except a possible factor of 4.*
3. *E has j-invariant $j = \frac{(\alpha^2-48)^3}{(\alpha-8)(\alpha+8)}$, where $\alpha \in \mathbb{Z}$, $\alpha \pm 8$ are squarefree.*

Let θ be a root of Ψ_3. If any of the above hypotheses holds, then the third partial torsion field, $\mathbb{Q}(\theta)$, is monogenic with a generator given by a root of $T^4 - 6T^2 - \alpha T - 3$. Note the generator of the power basis is **not** *θ. Moreover, $\mathbb{Q}(\theta)$ has discriminant $-27(\alpha-8)^2(\alpha+8)^2$.*

Why $T^4 - 6T^2 - \alpha T - 3$?

Often, if you want to look at elliptic curves with 4-torsion over $\mathbb{Q}$, you look at the curve

$$E : y^2 + (\alpha + 8\beta)xy + \beta(\alpha + 8\beta)^2 y = x^3 + \beta(\alpha + 8\beta)x^2.$$

This parametrization is called Tate's normal form.

Why $T^4 - 6T^2 - \alpha T - 3$?

Often, if you want to look at elliptic curves with 4-torsion over $\mathbb{Q}$, you look at the curve

$$E : y^2 + (\alpha + 8\beta)xy + \beta(\alpha + 8\beta)^2 y = x^3 + \beta(\alpha + 8\beta)x^2.$$

This parametrization is called Tate's normal form. Here $(0, 0)$ has order 4 and

$$\begin{aligned}\Psi_3 =& 3x^4 + \left((\alpha + 8\beta)^2 + 4\beta(\alpha + 8\beta)\right) x^3 + 3\beta(\alpha + 8\beta)^3 x^2 \\ &+ 3\beta^2(\alpha + 8\beta)^4 x + \beta^3(\alpha + 8\beta)^5.\end{aligned}$$

Why $T^4 - 6T^2 - \alpha T - 3$?

Often, if you want to look at elliptic curves with 4-torsion over $\mathbb{Q}$, you look at the curve

$$E : y^2 + (\alpha + 8\beta)xy + \beta(\alpha + 8\beta)^2 y = x^3 + \beta(\alpha + 8\beta)x^2.$$

This parametrization is called Tate's normal form. Here $(0, 0)$ has order 4 and

$$\begin{aligned}\Psi_3 =& 3x^4 + \left((\alpha + 8\beta)^2 + 4\beta(\alpha + 8\beta)\right) x^3 + 3\beta(\alpha + 8\beta)^3 x^2 \\ & + 3\beta^2(\alpha + 8\beta)^4 x + \beta^3(\alpha + 8\beta)^5.\end{aligned}$$

However, we found the model that worked best for us was the Fueter form:

$$T_1^2 = 4T^3 + \frac{\alpha}{\beta} T^2 + 4T.$$

Here the identity is $(0, 0)$ and $\left(1, \sqrt{8 + \frac{\alpha}{\beta}}\right)$ is a point of order 4.

Why $T^4 - 6T^2 - \alpha T - 3$?

Recall

$$\begin{aligned}\Psi_3 =& 3x^4 + \left((\alpha+8\beta)^2 + 4\beta(\alpha+8\beta)\right)x^3 + 3\beta(\alpha+8\beta)^3x^2 \\ &+ 3\beta^2(\alpha+8\beta)^4x + \beta^3(\alpha+8\beta)^5.\end{aligned}$$

Why $T^4 - 6T^2 - \alpha T - 3$?

Recall

$$\begin{aligned}\Psi_3 =& 3x^4 + \left((\alpha+8\beta)^2 + 4\beta(\alpha+8\beta)\right)x^3 + 3\beta(\alpha+8\beta)^3x^2 \\ &+ 3\beta^2(\alpha+8\beta)^4x + \beta^3(\alpha+8\beta)^5.\end{aligned}$$

When we change to the Fueter form Ψ_3 becomes $T^4 - 6T^2 - \dfrac{\alpha}{\beta}T - 3$.

Why care?

Why care?

Hasse's problem: When is $\mathbb{Q}(\theta)$ monogenic?

Why care?

Hasse's problem: When is $\mathbb{Q}(\theta)$ monogenic?

Torsion fields, $\mathbb{Q}(E[m])$, are a generalization of cyclotomic fields. Cyclotomic fields and their maximal real subfields are monogenic. We have class field theory. Cyclotomic fields have very nice formulas for ramification and for the field discriminant.

Why care?

Hasse's problem: When is $\mathbb{Q}(\theta)$ monogenic?

Torsion fields, $\mathbb{Q}(E[m])$, are a generalization of cyclotomic fields. Cyclotomic fields and their maximal real subfields are monogenic. We have class field theory. Cyclotomic fields have very nice formulas for ramification and for the field discriminant.

Torsion on Elliptic Curves in general: Given a Galois group or a degree, what torsion subgroups can elliptic curves over number fields with that Galois group or that degree have?

Proof Ideas

The Montes Algorithm

Let $f(x)$ be a monic, irreducible, integer polynomial with root θ and let p be a prime. The Montes algorithm takes in $f(x)$ and through successive reductions and expansions tells us about $v_p\left(\left[\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]\right]\right)$.

The Montes Algorithm

Let $f(x)$ be a monic, irreducible, integer polynomial with root θ and let p be a prime. The Montes algorithm takes in $f(x)$ and through successive reductions and expansions tells us about $v_p\left(\left[\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]\right]\right)$.

Recall,

$$\operatorname{disc}\left(\mathbb{Q}(\theta)\right) \cdot \left[\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]\right]^2 = \operatorname{disc}(f).$$

The Montes Algorithm

Let $f(x)$ be a monic, irreducible, integer polynomial with root θ and let p be a prime. The Montes algorithm takes in $f(x)$ and through successive reductions and expansions tells us about $v_p\left(\left[\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]\right]\right)$.

Recall,

$$\operatorname{disc}\left(\mathbb{Q}(\theta)\right) \cdot \left[\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]\right]^2 = \operatorname{disc}(f).$$

In particular,

$$v_p\left(\operatorname{disc}(\mathbb{Q}(\theta))\right) + 2v_p\left(\left[\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]\right]\right) = v_p\left(\operatorname{disc}(f)\right).$$

The Montes Algorithm

Example: Consider $x^4 + 9x + 9$ and $p = 3$.

The Montes Algorithm

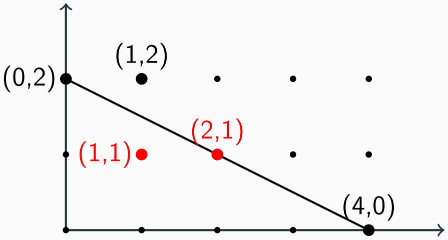
Example: Consider $x^4 + 9x + 9$ and $p = 3$. We reduce modulo 3 and obtain x^4.

The Montes Algorithm

Example: Consider $x^4 + 9x + 9$ and $p = 3$. We reduce modulo 3 and obtain x^4. The x-adic development is again $x^4 + 9x + 9$.

The Montes Algorithm

Example: Consider $x^4 + 9x + 9$ and $p = 3$. We reduce modulo 3 and obtain x^4. The x-adic development is again $x^4 + 9x + 9$. Now the x-Newton polygon is:



The x-Newton polygon

The Idea

We know the discriminant of Ψ_n is divisible only by primes dividing n and primes at which the elliptic curve in question has bad reduction. This gives us a small list of primes for which monogeneity can fail.

The Idea

We know the discriminant of Ψ_n is divisible only by primes dividing n and primes at which the elliptic curve in question has bad reduction. This gives us a small list of primes for which monogeneity can fail.

The Montes algorithm gives us a tool to deal with our small list of potentially problematic primes, but knowing the valuations of every coefficient of Ψ_n is not easy.

The Idea

We know the discriminant of Ψ_n is divisible only by primes dividing n and primes at which the elliptic curve in question has bad reduction. This gives us a small list of primes for which monogeneity can fail.

The Montes algorithm gives us a tool to deal with our small list of potentially problematic primes, but knowing the valuations of every coefficient of Ψ_n is not easy.

However, if the constant coefficient has valuation 1 we don't need to know about the other coefficients.

Valuations of Division Polynomials

Stange has a paper where the valuations of the division polynomials evaluated at a point are explicitly computed. The valuations depend on the reduction data of the elliptic curve.

Valuations of Division Polynomials

Stange has a paper where the valuations of the division polynomials evaluated at a point are explicitly computed. The valuations depend on the reduction data of the elliptic curve.

We want to plug any point $P \in E(\overline{\mathbb{Q}})$ with $x(P) = 0$ into Ψ_n so we can find the valuation of the constant coefficient.

Tate's Algorithm

Given a curve

$$E : y^2 + (\alpha + 8\beta)xy + \beta(\alpha + 8\beta)^2 y = x^3 + \beta(\alpha + 8\beta)x^2$$

in Tate's normal form we apply Tate's algorithm to understand the reduction type of E in terms of α and β.

Change Coordinates

Finally, we change coordinates to get to the Fueter form of the curve. The change of coordinates is...

Change Coordinates

Finally, we change coordinates to get to the Fueter form of the curve. The change of coordinates is...

$$(x, y) = \left(\frac{a\beta}{T} - a\beta, \frac{1}{2} \left(\frac{(a\beta)^{\frac{3}{2}} T_1}{T^2} - \frac{a^2\beta}{T} \right) \right).$$

Change Coordinates

Finally, we change coordinates to get to the Fueter form of the curve. The change of coordinates is...

$$(x, y) = \left(\frac{a\beta}{T} - a\beta, \frac{1}{2} \left(\frac{(a\beta)^{\frac{3}{2}} T_1}{T^2} - \frac{a^2\beta}{T} \right) \right).$$

We apply the Montes algorithm to obtain the result. We've also shown that the odd Fueter division polynomials don't yield monogenic fields for $n > 3$.

Further Questions

Further Questions

Can we use the Montes algorithm and explicit formulas for the discriminant of a polynomial to find other monogenic families?

Further Questions

Can an in-depth analysis of division polynomials, perhaps in conjunction with the Montes algorithm, shed light on some properties of torsion fields and torsion point fields?

Thank You

Thank you for listening. Preprints of this work and some of the other work mentioned is available on my website:

http://math.colorado.edu/∼hwsmith/index.html