Non-monogenic Division Fields of Elliptic Curves

Hanson Smith

University of Colorado, Boulder

Table of contents

Motivation and Background

$\mathbb{G}_m$ torsion fields (cyclotomic fields)

Consider $\mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^*$.

$\mathbb{G}_m$ torsion fields (cyclotomic fields)

Consider $\mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^*$.

The $\mathbb{G}_m(\mathbb{Q})$ torsion points are the roots of unity, the solutions to $x^n - 1$.

$\mathbb{G}_m$ torsion fields (cyclotomic fields)

Consider $\mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^*$.

The $\mathbb{G}_m(\mathbb{Q})$ torsion points are the roots of unity, the solutions to $x^n - 1$.

One way to study the $\mathbb{G}_m(\mathbb{Q})$ torsion points is to look at the n^{th} $\mathbb{G}_m(\mathbb{Q})$ torsion field, $\mathbb{Q}\left(\mathbb{G}_m(\mathbb{Q})[n]\right) = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity.

$\mathbb{G}_m$ torsion fields (cyclotomic fields)

Consider $\mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^*$.

The $\mathbb{G}_m(\mathbb{Q})$ torsion points are the roots of unity, the solutions to $x^n - 1$.

One way to study the $\mathbb{G}_m(\mathbb{Q})$ torsion points is to look at the n^{th} $\mathbb{G}_m(\mathbb{Q})$ torsion field, $\mathbb{Q}\left(\mathbb{G}_m(\mathbb{Q})[n]\right) = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity. We will use *torsion field* and *division field* interchangeably.

$\mathbb{G}_m$ torsion fields (cyclotomic fields)

What does $\mathbb{Q}(\zeta_n)$ look like?

$\mathbb{G}_m$ torsion fields (cyclotomic fields)

What does $\mathbb{Q}(\zeta_n)$ look like?

The discriminant is a power of n, so primes dividing n are the only ramified primes.

$\mathbb{G}_m$ torsion fields (cyclotomic fields)

What does $\mathbb{Q}(\zeta_n)$ look like?

The discriminant is a power of n, so primes dividing n are the only ramified primes.

The residue class degree of a prime p not dividing n is the least positive integer f such that $p^f \equiv 1 \bmod n$.

$\mathbb{G}_m$ torsion fields (cyclotomic fields)

What does $\mathbb{Q}(\zeta_n)$ look like?

The discriminant is a power of n, so primes dividing n are the only ramified primes.

The residue class degree of a prime p not dividing n is the least positive integer f such that $p^f \equiv 1 \bmod n$.

The ring of integers is $\mathbb{Z}[\zeta_n]$.

Elliptic Curves

You can think of an elliptic curve E as the solutions to an equation of the form $y^2 = x^3 + Ax + B$.

Elliptic Curves

You can think of an elliptic curve E as the solutions to an equation of the form $y^2 = x^3 + Ax + B$.

Elliptic curves look like this.

Elliptic Curves

You can think of an elliptic curve E as the solutions to an equation of the form $y^2 = x^3 + Ax + B$.

Elliptic curves look like this.

One reason that elliptic curves are special is the points of an elliptic curve form an abelian group.

Elliptic Curves

If K is a number field then, $E(K) \cong \mathbb{Z}^r \times E(K)_{\text{tors}}$.

Elliptic Curves

If K is a number field then, $E(K) \cong \mathbb{Z}^r \times E(K)_{\text{tors}}$.

The integer r is called the *rank* and $E(K)_{\text{tors}}$ is called the *torsion subgroup*.

Elliptic Curves

If K is a number field then, $E(K) \cong \mathbb{Z}^r \times E(K)_{\text{tors}}$.

The integer r is called the *rank* and $E(K)_{\text{tors}}$ is called the *torsion subgroup*.

We denote the n-torsion points of an elliptic curve E by $E[n]$. Over $\mathbb{C}$ one has $E(\mathbb{C})[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Elliptic Curves

If K is a number field then, $E(K) \cong \mathbb{Z}^r \times E(K)_{\text{tors}}$.

The integer r is called the *rank* and $E(K)_{\text{tors}}$ is called the *torsion subgroup*.

We denote the n-torsion points of an elliptic curve E by $E[n]$. Over $\mathbb{C}$ one has $E(\mathbb{C})[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

We will be looking at the n-torsion fields of an elliptic curve: $\mathbb{Q}(E[n])$.

Comparing $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(E[n])$

The only ramified primes in $\mathbb{Q}(E[n])$ are the primes dividing n and the primes dividing the discriminant of E.

Comparing $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(E[n])$

The only ramified primes in $\mathbb{Q}(E[n])$ are the primes dividing n and the primes dividing the discriminant of E.

Let a_p be the trace of Frobenius at p, let b_p be the index $[\mathcal{O}_K : \mathrm{End}_{\mathbb{F}_p}(E)]$, and write Δ_{End} for the discriminant of $\mathrm{End}_{\mathbb{F}_p}(E)$. Consider now the matrix

$$\sigma_p = \begin{bmatrix} \frac{a_p + b_p\delta_{\mathrm{End}}}{2} & b_p \\ \frac{b_p(\Delta_{\mathrm{End}} - \delta_{\mathrm{End}})}{4} & \frac{a_p - b_p\delta_{\mathrm{End}}}{2} \end{bmatrix}, \tag{1}$$

where $\delta_{\mathrm{End}} = 0, 1$ according to whether $\Delta_{\mathrm{End}} \equiv 0, 1$ modulo 4.

Comparing $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(E[n])$

The only ramified primes in $\mathbb{Q}(E[n])$ are the primes dividing n and the primes dividing the discriminant of E.

Let a_p be the trace of Frobenius at p, let b_p be the index $[\mathcal{O}_K : \mathrm{End}_{\mathbb{F}_p}(E)]$, and write Δ_{End} for the discriminant of $\mathrm{End}_{\mathbb{F}_p}(E)$. Consider now the matrix

$$\sigma_p = \begin{bmatrix} \frac{a_p + b_p\delta_{\mathrm{End}}}{2} & b_p \\ \frac{b_p(\Delta_{\mathrm{End}} - \delta_{\mathrm{End}})}{4} & \frac{a_p - b_p\delta_{\mathrm{End}}}{2} \end{bmatrix}, \tag{1}$$

where $\delta_{\mathrm{End}} = 0, 1$ according to whether $\Delta_{\mathrm{End}} \equiv 0, 1$ modulo 4.

Duke and Tóth: Suppose n is prime to p. When reduced modulo n, the matrix σ_p yields a global representation of the Frobenius class over p in $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

Comparing $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(E[n])$

The only ramified primes in $\mathbb{Q}(E[n])$ are the primes dividing n and the primes dividing the discriminant of E.

Let a_p be the trace of Frobenius at p, let b_p be the index $[\mathcal{O}_K : \mathrm{End}_{\mathbb{F}_p}(E)]$, and write Δ_{End} for the discriminant of $\mathrm{End}_{\mathbb{F}_p}(E)$. Consider now the matrix

$$\sigma_p = \begin{bmatrix} \dfrac{a_p + b_p\delta_{\mathrm{End}}}{2} & b_p \\ \dfrac{b_p(\Delta_{\mathrm{End}} - \delta_{\mathrm{End}})}{4} & \dfrac{a_p - b_p\delta_{\mathrm{End}}}{2} \end{bmatrix}, \tag{1}$$

where $\delta_{\mathrm{End}} = 0, 1$ according to whether $\Delta_{\mathrm{End}} \equiv 0, 1$ modulo 4.

Duke and Tóth: Suppose n is prime to p. When reduced modulo n, the matrix σ_p yields a global representation of the Frobenius class over p in $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. In particular, the order of σ_p modulo n is the residue class degree of p in $\mathbb{Q}(E[n])$.

Comparing $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(E[n])$

Motivating question: Can I write the ring of integers $\mathcal{O}_{\mathbb{Q}(E[n])}$ as $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathbb{Q}(E[n])$?

Comparing $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(E[n])$

Motivating question: Can I write the ring of integers $\mathcal{O}_{\mathbb{Q}(E[n])}$ as $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathbb{Q}(E[n])$?

In other words, when is $\mathbb{Q}(E[n])$ *monogenic*?

Comparing $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(E[n])$

Motivating question: Can I write the ring of integers $\mathcal{O}_{\mathbb{Q}(E[n])}$ as $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathbb{Q}(E[n])$?

In other words, when is $\mathbb{Q}(E[n])$ *monogenic*?

As we've seen, all $\mathbb{G}_m(\mathbb{Q})$ torsion fields are monogenic.

Comparing $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(E[n])$

Motivating question: Can I write the ring of integers $\mathcal{O}_{\mathbb{Q}(E[n])}$ as $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathbb{Q}(E[n])$?

In other words, when is $\mathbb{Q}(E[n])$ *monogenic*?

As we've seen, all $\mathbb{G}_m(\mathbb{Q})$ torsion fields are monogenic.

Gonzáles-Jiménez and Lozano-Robledo show that $\mathbb{Q}(E[n])$ coincides with $\mathbb{Q}(\zeta_n)$ sometimes. In particular when $n = 2, 3, 4$, and 5 this can happen.

Results

Main Result

There are a lot of torsion fields $\mathbb{Q}(E[n])$ that are not monogenic

Main Result

There are a lot of torsion fields $\mathbb{Q}(E[n])$ that are not monogenic

Theorem (Smith)
If E is an elliptic curve over $\mathbb{Q}$ whose reduction at the prime 2 has trace of Frobenius a_2 and such that, for one of the n listed on the following slide, the Galois representation

$$\rho_{E,n} : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

is surjective. Then $\mathbb{Q}(E[n])$ is not monogenic. Moreover, 2 is an essential discriminant divisor of $\mathbb{Q}(E[n])$.

Results for $p = 2$

a_2	σ_2	non-monogenic n
1	$\begin{bmatrix} 4 & -14 \\ 1 & -3 \end{bmatrix}$	11
-1	$\begin{bmatrix} 3 & -14 \\ 1 & -4 \end{bmatrix}$	11, 23
2	$\begin{bmatrix} 3 & -5 \\ 1 & -1 \end{bmatrix}$	5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819
-2	$\begin{bmatrix} 1 & -5 \\ 1 & -3 \end{bmatrix}$	5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819

Table 1: Using the splitting of 2 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$.

Results for $p = 3$

a_3	σ_3	non-monogenic n
1	$\begin{bmatrix} 6 & -33 \\ 1 & -5 \end{bmatrix}$	5, 40
-1	$\begin{bmatrix} 5 & -33 \\ 1 & -6 \end{bmatrix}$	5, 23, 40
2	$\begin{bmatrix} 5 & -18 \\ 1 & -3 \end{bmatrix}$	4, 11, 22, 136, 272
-2	$\begin{bmatrix} 3 & -18 \\ 1 & -5 \end{bmatrix}$	4, 22, 136, 272
3	$\begin{bmatrix} 3 & -3 \\ 1 & 0 \end{bmatrix}$	7, 14, 28, 52, 56, 91, 104, 182, 259, 266, 364, 518, 532, 703, 728, 949
-3	$\begin{bmatrix} 0 & -3 \\ 1 & -3 \end{bmatrix}$	7, 14, 28, 52, 56, 91, 104, 182, 259, 266, 364, 518, 532, 703, 728, 949

Table 2: Using the splitting of 3 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$.

Results for $p = 5$

a_5	b_5	σ_5	non-monogenic n
1	1	$\begin{bmatrix} 10 & -95 \\ 1 & -9 \end{bmatrix}$	11, 28, 56
-1	1	$\begin{bmatrix} 9 & -95 \\ 1 & -10 \end{bmatrix}$	28, 56
2	1	$\begin{bmatrix} 9 & -68 \\ 1 & -7 \end{bmatrix}$	$\emptyset$
-2	1	$\begin{bmatrix} 7 & -68 \\ 1 & -9 \end{bmatrix}$	$\emptyset$
2	2	$\begin{bmatrix} 5 & -10 \\ 2 & -3 \end{bmatrix}$	4, 8, 48
-2	2	$\begin{bmatrix} 3 & -10 \\ 2 & -5 \end{bmatrix}$	4, 8, 48
3	1	$\begin{bmatrix} 7 & -33 \\ 1 & -4 \end{bmatrix}$	3, 18, 24, 36, 72
-3	1	$\begin{bmatrix} 4 & -33 \\ 1 & -7 \end{bmatrix}$	3, 18, 24, 36, 72
4	1	$\begin{bmatrix} 4 & -5 \\ 1 & 0 \end{bmatrix}$	8, 48
-4	1	$\begin{bmatrix} 0 & -5 \\ 1 & -4 \end{bmatrix}$	8, 48

Table 3: Using the splitting of 5 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$.

Proof Ingredients and Ideas

Dedekind and Kummer

Theorem (Dedekind building on work of Kummer)
Let $f \in \mathbb{Z}[x]$ be monic and irreducible and let $L = \mathbb{Q}(\alpha)$ where α is a root of f. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$, the the factorization of p in $\mathcal{O}_L$ mirrors the factorization of f modulo p.

Dedekind and Kummer

Theorem (Dedekind building on work of Kummer)
Let $f \in \mathbb{Z}[x]$ be monic and irreducible and let $L = \mathbb{Q}(\alpha)$ where α is a root of f. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$, the the factorization of p in $\mathcal{O}_L$ mirrors the factorization of f modulo p. That is,

$$f(x) \equiv \phi_1(x)^{e_1} \cdots \phi_r(x)^{e_r} \text{ and } p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Dedekind and Kummer

Theorem (Dedekind building on work of Kummer)
Let $f \in \mathbb{Z}[x]$ be monic and irreducible and let $L = \mathbb{Q}(\alpha)$ where α is a root of f. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$, the the factorization of p in $\mathcal{O}_L$ mirrors the factorization of f modulo p. That is,

$$f(x) \equiv \phi_1(x)^{e_1} \cdots \phi_r(x)^{e_r} \text{ and } p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Consider $\mathbb{Q}(\alpha)$ where α is a root of $x^3 - x^2 - 2x - 8$.

Dedekind and Kummer

Theorem (Dedekind building on work of Kummer)
Let $f \in \mathbb{Z}[x]$ be monic and irreducible and let $L = \mathbb{Q}(\alpha)$ where α is a root of f. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$, the the factorization of p in $\mathcal{O}_L$ mirrors the factorization of f modulo p. That is,

$$f(x) \equiv \phi_1(x)^{e_1} \cdots \phi_r(x)^{e_r} \text{ and } p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Consider $\mathbb{Q}(\alpha)$ where α is a root of $x^3 - x^2 - 2x - 8$. SageMath:

$$2 = \left(\frac{\alpha^2 + \alpha}{2} + 1\right)\left(\alpha^2 + 2\alpha + 3\right)\left(\frac{3\alpha^2 + 5\alpha}{2} + 4\right).$$

Dedekind and Kummer

Theorem (Dedekind building on work of Kummer)
Let $f \in \mathbb{Z}[x]$ be monic and irreducible and let $L = \mathbb{Q}(\alpha)$ where α is a root of f. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$, the the factorization of p in $\mathcal{O}_L$ mirrors the factorization of f modulo p. That is,

$$f(x) \equiv \phi_1(x)^{e_1} \cdots \phi_r(x)^{e_r} \text{ and } p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Consider $\mathbb{Q}(\alpha)$ where α is a root of $x^3 - x^2 - 2x - 8$. SageMath:

$$2 = \left(\frac{\alpha^2 + \alpha}{2} + 1\right)\left(\alpha^2 + 2\alpha + 3\right)\left(\frac{3\alpha^2 + 5\alpha}{2} + 4\right).$$

I need to find $f(x)$ with root θ so that $2 \nmid \left[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\theta]\right]$.

Dedekind and Kummer

Theorem (Dedekind building on work of Kummer)
Let $f \in \mathbb{Z}[x]$ be monic and irreducible and let $L = \mathbb{Q}(\alpha)$ where α is a root of f. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$, the the factorization of p in $\mathcal{O}_L$ mirrors the factorization of f modulo p. That is,

$$f(x) \equiv \phi_1(x)^{e_1} \cdots \phi_r(x)^{e_r} \text{ and } p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Consider $\mathbb{Q}(\alpha)$ where α is a root of $x^3 - x^2 - 2x - 8$. SageMath:

$$2 = \left(\frac{\alpha^2 + \alpha}{2} + 1\right)\left(\alpha^2 + 2\alpha + 3\right)\left(\frac{3\alpha^2 + 5\alpha}{2} + 4\right).$$

I need to find $f(x)$ with root θ so that $2 \nmid \left[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\theta]\right]$. In particular, f needs to split into 3 distinct linear factors modulo 2...

An Example

Suppose E is an elliptic curve with $a_2 = 1$.

An Example

Suppose E is an elliptic curve with $a_2 = 1$.

The discriminant of the characteristic polynomial of Frobenius, $x^2 - x + 2$, is -7.

An Example

Suppose E is an elliptic curve with $a_2 = 1$.

The discriminant of the characteristic polynomial of Frobenius, $x^2 - x + 2$, is -7.

Letting π denote the Frobenius endomorphism of E over $\mathbb{F}_2$, we have $\mathrm{End}_{\mathbb{F}_2}(E) = \mathbb{Z}[\pi] = \mathcal{O}_{\mathbb{Q}(\pi)}$.

An Example

Suppose E is an elliptic curve with $a_2 = 1$.

The discriminant of the characteristic polynomial of Frobenius, $x^2 - x + 2$, is -7.

Letting π denote the Frobenius endomorphism of E over $\mathbb{F}_2$, we have $\mathrm{End}_{\mathbb{F}_2}(E) = \mathbb{Z}[\pi] = \mathcal{O}_{\mathbb{Q}(\pi)}$.

Combining all this information, we see Duke and Tóth's matrix representing π is

$$\sigma_2 = \begin{bmatrix} 8/2 & (-7 \cdot 8)/4 \\ 1 & -6/2 \end{bmatrix} = \begin{bmatrix} 4 & -14 \\ 1 & -3 \end{bmatrix}.$$

An Example

Suppose E is an elliptic curve with $a_2 = 1$.

The discriminant of the characteristic polynomial of Frobenius, $x^2 - x + 2$, is -7.

Letting π denote the Frobenius endomorphism of E over $\mathbb{F}_2$, we have $\mathrm{End}_{\mathbb{F}_2}(E) = \mathbb{Z}[\pi] = \mathcal{O}_{\mathbb{Q}(\pi)}$.

Combining all this information, we see Duke and Tóth's matrix representing π is

$$\sigma_2 = \begin{bmatrix} 8/2 & (-7 \cdot 8)/4 \\ 1 & -6/2 \end{bmatrix} = \begin{bmatrix} 4 & -14 \\ 1 & -3 \end{bmatrix}.$$

Denote the order of σ_2 modulo n by $\mathrm{ord}\,(\sigma_2, n)$. This is the residue class degree of 2 in $\mathbb{Q}(E[n])$.

An Example

Generically, we expect the degree of $\mathbb{Q}(E[n])$ over $\mathbb{Q}$ to be $|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|$.

An Example

Generically, we expect the degree of $\mathbb{Q}(E[n])$ over $\mathbb{Q}$ to be $|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|$.

Thus 2 will split into $\dfrac{|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\operatorname{ord}(\sigma_2, n)}$ primes in $\mathbb{Q}(E[n])$.

An Example

Generically, we expect the degree of $\mathbb{Q}(E[n])$ over $\mathbb{Q}$ to be $|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|$.

Thus 2 will split into $\dfrac{|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\operatorname{ord}(\sigma_2, n)}$ primes in $\mathbb{Q}(E[n])$.

The number of irreducible polynomials of degree m in $\mathbb{F}_p[x]$ is $\dfrac{1}{m}\sum_{d|m} p^d \mu\left(\dfrac{m}{d}\right)$.

An Example

Generically, we expect the degree of $\mathbb{Q}(E[n])$ over $\mathbb{Q}$ to be $|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|$.

Thus 2 will split into $\dfrac{|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\operatorname{ord}(\sigma_2, n)}$ primes in $\mathbb{Q}(E[n])$.

The number of irreducible polynomials of degree m in $\mathbb{F}_p[x]$ is
$\dfrac{1}{m}\displaystyle\sum_{d|m} p^d \mu\left(\frac{m}{d}\right)$.

With Dedekind's Theorem in mind, we compare $\dfrac{|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\operatorname{ord}(\sigma_2, n)}$ and

$$\frac{1}{\operatorname{ord}(\sigma_2, n)} \sum_{d|\operatorname{ord}(\sigma_2,n)} 2^d \mu\left(\frac{\operatorname{ord}(\sigma_2, n)}{d}\right).$$

An Example

If the number of irreducible polynomial of degree $\operatorname{ord}(\sigma_2, n)$ in $\mathbb{F}_2[x]$ is less than $\dfrac{|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\operatorname{ord}(\sigma_2, n)}$, then 2 must divide the index of any monogenic order in $\mathcal{O}_{\mathbb{Q}(E[n])}$.

An Example

If the number of irreducible polynomial of degree $\mathrm{ord}(\sigma_2, n)$ in $\mathbb{F}_2[x]$ is less than $\dfrac{|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\mathrm{ord}(\sigma_2, n)}$, then 2 must divide the index of any monogenic order in $\mathcal{O}_{\mathbb{Q}(E[n])}$.

We find that σ_2 has order 10 modulo 11. We compute that 2 splits into 1320 primes in $\mathbb{Q}(E[11])$, but there are only 99 irreducible polynomials of degree 10 in $\mathbb{F}_2[x]$.

Thus if E is an elliptic curve over $\mathbb{Q}$ with $a_2 = 1$ and with $[\mathbb{Q}(E[11]) : \mathbb{Q}] = |\operatorname{GL}_2(\mathbb{Z}/11\mathbb{Z})|$, then $\mathbb{Q}(E[11])$ is not monogenic.

Further Questions

Further Questions

Abelian varieties?

Further Questions

Abelian varieties?

Analogs of the this presentation hold when A is a simple, ordinary abelian variety such that $\mathrm{End}_{\mathbb{F}_p}(A) \cong \mathbb{Z}[\pi, v]$.

Thank You

Thank you for listening. Please send me an email at hanson.smith@colorado.edu if you have any questions that aren't answered here.