



# Monogenicity\* and Torsion

---

Hanson Smith

University of Connecticut

# Table of contents

1. Background and Motivation
2. Radicals
3. Division Field Motivation
4. Results for Division Fields of Elliptic Curves
5. Results for Abelian Varieties of Dimension  $> 1$

# Background and Motivation

---

# Monogenicity

Let  $f(x) \in \mathbb{Z}[x]$  be monic irreducible polynomial of degree  $n$ . Suppose  $\alpha$  is a root of  $f(x)$  and consider  $\mathbb{Q}(\alpha)$ . We call the field  $\mathbb{Q}(\alpha)$  a *number field*. You can think of a number field as a generalization of  $\mathbb{Q}$ . Number theorists love  $\mathbb{Z}$ , and  $\mathbb{Z}$  lives in  $\mathbb{Q}$ , so what is the analogue of  $\mathbb{Z}$  living in  $\mathbb{Q}(\alpha)$ ? Define *the ring of integers of  $\mathbb{Q}(\alpha)$* , denoted  $\mathcal{O}_{\mathbb{Q}(\alpha)}$ , to be the set of all solutions to monic polynomials in  $\mathbb{Z}[x]$  that are in  $\mathbb{Q}(\alpha)$ .

Our question today will be, When is  $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\beta]$  for some  $\beta \in \mathbb{Q}(\alpha)$ ? To be more explicit, Is there a  $\beta \in \mathbb{Q}(\alpha)$  such that

$$\mathcal{O}_{\mathbb{Q}(\alpha)} = \{a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-1}\beta^{n-1} : a_i \in \mathbb{Z}\}?$$

When this is the case we say  $\mathbb{Q}(\alpha)$  is *monogenic* or  $\mathcal{O}_{\mathbb{Q}(\alpha)}$  admits a *power integral basis*.

Let  $L/K$  be an extension of number fields of degree  $n$  with respective rings of integers  $\mathcal{O}_L$  and  $\mathcal{O}_K$ . We say  $L$  is *monogenic over  $K$*  or  $\mathcal{O}_L$  *admits a power  $\mathcal{O}_K$ -integral basis* if  $\mathcal{O}_L = \mathcal{O}_K[\alpha]$  for some  $\alpha \in L$ . More explicitly,  $\{1, \alpha, \dots, \alpha^{n-1}\}$  is an  $\mathcal{O}_K$ -basis for the  $\mathcal{O}_K$ -module  $\mathcal{O}_L$ .

Let's get our hands dirty with this definition to see why it is natural and important!

# Monogenicity of Quadratics

Take  $\mathbb{Q}(\sqrt{d})$ , with  $d$  square-free. What is the ring of integers of this field? What are the solutions to monic polynomials in  $\mathbb{Z}[x]$ ?

Take an arbitrary element  $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ . We compute

$$f(x) = \left(x - (a + b\sqrt{d})\right) \left(x - (a - b\sqrt{d})\right) = x^2 - 2ax + a^2 - b^2d.$$

In order for  $f(x)$  to be in  $\mathbb{Z}[x]$ , we need  $2a \in \mathbb{Z}$ . If  $a \in \mathbb{Z}$ , then  $b \in \mathbb{Z}$  in order to have  $f(x) \in \mathbb{Z}[x]$ . But, if  $a = \frac{a_0}{2}$ , then a bit of arithmetic modulo 4 shows that we need  $b = \frac{b_0}{2}$  and  $(a_0^2 - b_0^2d)/4 \in \mathbb{Z}$  in order to have  $a^2 - b^2d \in \mathbb{Z}$ . For this case to work out, it is necessary and sufficient that  $d \equiv 1 \pmod{4}$ . Thus the ring of integers of  $\mathbb{Q}(\sqrt{d})$  is  $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$  if  $d \equiv 1 \pmod{4}$  and  $\mathbb{Z}[\sqrt{d}]$  otherwise. In either case,  $\mathbb{Q}(\sqrt{d})$  is monogenic, but  $\sqrt{d}$  generates a power integral basis if and only if  $d \not\equiv 1 \pmod{4}$ . The key here that we will generalize later on is  $d$  is not a square modulo  $2^2$ .

# Monogenicity of Cyclotomics

Let's imagine we are building algebraic number theory. We want to understand number fields and rings of integers. We've already figured out a few things about  $\mathbb{Q}(\sqrt{d})$ . Where do we go next? How about we look at number fields generated by really nice polynomials? What about the polynomial  $x^n - 1$ ?

Let  $\zeta_n$  be a primitive  $n^{\text{th}}$  root of unity, so  $\zeta_n^n = 1$ , but  $\zeta_n^k \neq 1$  for  $1 \leq k < n$ . Let's look at  $\mathbb{Q}(\zeta_n)$ . It is a bit more difficult than in the quadratic case, but one can show that the ring of integers of  $\mathbb{Q}(\zeta_n)$  is  $\mathbb{Z}[\zeta_n]$ !

**Flippant Conjecture:** Every number field is monogenic!

# “All that glistens is not gold.”

Does this always happen? When one is learning (or discovering) algebraic number theory, they might be tempted to think every extension of  $\mathbb{Q}$  is monogenic. It works for the first two families of number fields we encounter, so maybe we expect it always happens.

*Expectation is the root of all heartache.*

- William Shakespeare



# Dedekind-Kummer Factorization

## Theorem (Dedekind building on work of Kummer)

Let  $f(x)$  be a monic, irreducible polynomial in  $\mathbb{Z}[x]$  with  $\alpha$  denoting a root. If  $p \in \mathbb{Z}$  is a prime that does not divide  $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$ , then the factorization of  $p$  in  $\mathcal{O}_{\mathbb{Q}(\alpha)}$  mirrors the factorization of  $f(x)$  in  $\mathbb{F}_p[x]$ .

That is,

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p} \quad \text{and} \quad (p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

For example, consider  $\mathbb{Q}(\alpha)$  where  $\alpha$  is a root of  $x^3 - x^2 - 2x - 8$ . Dedekind computed the factorization  $(2) = \mathfrak{p}_2 \mathfrak{p}_2' \mathfrak{p}_2''$ .

Thus, if this field is monogenic, there is a cubic polynomial that generates and has **three** distinct linear factors in  $\mathbb{F}_2[x]$ .

# Common Index Divisors

One can generalize Dedekind's example: If a prime  $p < n$  splits completely in an extension  $K/\mathbb{Q}$  of degree  $n$ , then  $K$  is not monogenic. [Hensel, 1894] builds on these ideas to show the following.

## Theorem

*Fix a prime  $p$ . The prime  $p$  divides  $[\mathcal{O}_K : \mathbb{Z}[\theta]]$  for every algebraic integer  $\theta$  generating  $K$  over  $\mathbb{Q}$  if and only if there is an integer  $f$  such that the number of prime ideal factors of  $p\mathcal{O}_K$  with inertia degree  $f$  is greater than the number of monic irreducibles of degree  $f$  in  $\mathbb{F}_p[x]$ .*

Any  $p$  satisfying this theorem is called a *common index divisor*. The terms 'essential discriminant divisor' and 'inessential discriminant divisor' also appear in the literature. The shortcomings of the English nomenclature likely come from what Neukirch [Neukirch, 1999, page 207] calls "the untranslatable German catch phrase [...] 'außerwesentliche Diskriminantenteile.'" Our nomenclature is closer to Fricke's 'ständiger Indexteiler.'

## Other Obstructions

It turns out that common index divisors are not the only obstruction to monogenicity:

**Example:** [Narkiewicz, 2004, Chapter 2.2.6] Consider the number field given by  $K = \mathbb{Q}(\sqrt[3]{7 \cdot 5^2}) = \mathbb{Q}(\sqrt[3]{5 \cdot 7^2})$ . The elements  $\{1, \sqrt[3]{7 \cdot 5^2}, \sqrt[3]{7^2 \cdot 5}\}$  form an integral basis for  $\mathcal{O}_K$ . For any fixed prime  $p$ , one can find  $\alpha \in \mathcal{O}_K$  such that  $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$  is not divisible by  $p$ ; however,  $K$  is not monogenic.

In fact, the index  $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$  can be described with a form, called the *index form*. In the example above it is  $5X_1^3 - 7X_2^3$ . We can consider it modulo 7 to see that there are no values for which the form is  $\pm 1$ .

# Radicals

---

# Radical (Pure) Motivation

Remember, the ring of integers of  $\mathbb{Q}(\sqrt{d})$  is  $\mathbb{Z}[\sqrt{d}]$  if and only if  $d$  is squarefree and  $d \not\equiv 1 \pmod{4}$ . Can we generalize?

[Westlund, 1910] computed the discriminant and an integral basis for the radical extensions  $\mathbb{Q}(\sqrt[p]{\alpha})$  over  $\mathbb{Q}$ , where  $\alpha \in \mathbb{Z}$  and  $p$  is a prime.

Westlund also identified when  $\sqrt[p]{\alpha}$  yields a power integral basis for  $\mathbb{Q}(\sqrt[p]{\alpha})$ . [Gassert, 2017] (see also [Jakhar et al., 2017]) gives necessary and sufficient conditions for the ring of integers of  $\mathbb{Q}(\sqrt[p]{\alpha})$  to be  $\mathbb{Z}[\sqrt[p]{\alpha}]$ . Having  $\sqrt[p]{\alpha}$  generate a power integral basis is dependent on the congruence

$$\alpha^p \equiv \alpha \pmod{p^2}, \tag{1}$$

where  $p$  divides  $n$ . Loosely speaking, Congruence (1) is an obstruction to  $\sqrt[p]{\alpha}$  generating a power integral basis.

# The Question

Let  $K$  be a number field and let  $x^n - \alpha$  be an irreducible element of  $K[x]$ . Consider  $L = K(\sqrt[n]{\alpha})$ .

**Question:** When does  $\sqrt[n]{\alpha}$  generate an  $\mathcal{O}_K$ -integral basis for  $\mathcal{O}_L$ ?

† It is worth noting that even the existence of a  $\mathcal{O}_K$ -integral basis is not guaranteed.

# A Digestible Corollary

## Theorem ([Smith, 2021b])

*Let  $p$  be an odd, rational prime and define  $K = \mathbb{Q}(\zeta_p)$ . Note  $(1 - \zeta_p)$  is the unique prime ideal of  $\mathcal{O}_K$  above  $p$ . Let  $\alpha \in \mathcal{O}_K$  and suppose that  $x^p - \alpha$  is irreducible in  $\mathcal{O}_K[x]$ . The ring of integers of  $K(\sqrt[p]{\alpha})$  is  $\mathcal{O}_K[\sqrt[p]{\alpha}]$  if and only if  $(\alpha)$  is a square-free ideal of  $\mathcal{O}_K$  and the congruence*

$$\alpha^p \equiv \alpha \pmod{(1 - \zeta_p)^2} \tag{2}$$

*is not satisfied.*

This is quite a contrast to the situation over  $\mathbb{Q}$ . [Gras, 1986] shows that the only abelian extensions of prime degree  $p \geq 5$  are maximal real subfields of cyclotomic fields.

# A Radical Result

For a prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$  dividing  $n$ , we write  $p$  for the residue characteristic and  $f$  for the residue class degree. If  $\mathfrak{p}$  divides  $n$ , we factor  $n = p^e m$  with  $\gcd(m, p) = 1$ . Let  $\varepsilon$  be congruent to  $e$  modulo  $f$  with  $1 \leq \varepsilon \leq f$  and define  $\beta$  to be  $\alpha$  to the power  $p^{f-\varepsilon}$ . By construction  $\beta$  is a  $p^e$ -th root of  $\alpha$  modulo  $\mathfrak{p}$ . Our congruence generalizes to

$$\alpha^{p^{f-\varepsilon+e}} = \beta^{p^e} \equiv \alpha \pmod{\mathfrak{p}^2}. \quad (3)$$

In the case where  $e \leq f$ , this is simply

$$\alpha^{p^f} \equiv \alpha \pmod{\mathfrak{p}^2}.$$

**Theorem** ([Smith, 2021b]) The ring of integers of  $K(\sqrt[n]{\alpha})$  is  $\mathcal{O}_K[\sqrt[n]{\alpha}]$  if and only if  $(\alpha)$  is a square-free ideal of  $\mathcal{O}_K$  and every prime  $\mathfrak{p}$  dividing  $n$  does not satisfy Congruence (3).



# A Very Recent Radical Result

**Theorem (S.)** If  $p$  is a common index divisor for  $\mathbb{Q}(\sqrt[n]{a})/\mathbb{Q}$ , then it is necessary that  $p \mid n$ .

If  $n = p^m$ , then for  $p$  to be a common index divisor it is necessary and sufficient that  $v_p(a^{p^m} - a) > p$ .

# Division Field Motivation

---

# Cyclotomic Fields ( $\mathbb{G}_m$ -Division Fields)

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

One way to study  $\mathbb{G}_m(\mathbb{Q})$  is to look at the  $n^{\text{th}}$   $\mathbb{G}_m(\mathbb{Q})$ -division field:  $\mathbb{Q}(\mathbb{G}_m(\mathbb{Q})[n]) = \mathbb{Q}(\zeta_n)$ . The 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  $p^f \equiv 1 \pmod{n}$ .

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

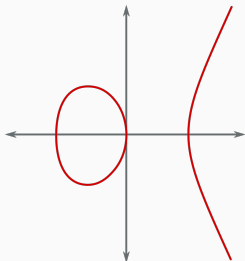
# Elliptic Curves

An *elliptic curve* is a smooth, projective curve of genus one with a specified point (the identity). You can think of an elliptic curve  $E$  as a donut.

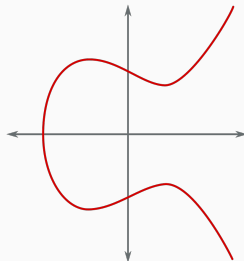


# Elliptic Curves

An *elliptic curve* is a smooth, projective curve of genus one with a specified point (the identity). You can think of an elliptic curve  $E$  as the solutions to an equation of the form  $y^2 = x^3 + Ax + B$ .



$$y^2 = x^3 - x$$



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

For this talk, the reason that we care about elliptic curves is the points of an elliptic curve form an abelian group.

# Elliptic Curves

Mordell-Weil: 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  $n$ -division fields of an elliptic curve:  $\mathbb{Q}(E[n])$ . The only ramified primes in  $\mathbb{Q}(E[n])$  are the primes dividing  $n$  and the primes dividing the discriminant of  $E$ .

## Splitting in $\mathbb{Q}(E[n])$

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

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

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

[Duke and Tóth, 2002]: Suppose  $n$  is prime to  $p$ . When reduced modulo  $n$ , the matrix  $\sigma_p$  yields a global representation of the Frobenius class over  $p$  in  $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ . In particular, the order of  $\sigma_p$  modulo  $n$  is the residue class degree of  $p$  in  $\mathbb{Q}(E[n])$ .

Motivating question: When is  $\mathbb{Q}(E[n])$  *monogenic*?

González-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.



# Monogenic 2-Division Fields

Legendre form,  $E_\lambda : y^2 = x(x-1)(x-\lambda)$ , requires solving

$$g_\lambda(\lambda) = \lambda^6 - 3\lambda^5 + \left(6 - \frac{j}{256}\right)\lambda^4 + \left(\frac{j}{128} - 7\right)\lambda^3 + \left(6 - \frac{j}{256}\right)\lambda^2 - 3\lambda + 1,$$

where  $j$  is the  $j$ -invariant of  $E_\lambda$ . Notice that  $\lambda \in \mathbb{Q}$  yields a family of elliptic curves with monogenic 2-division fields since  $\mathbb{Q}(E_\lambda[2]) = \mathbb{Q}$ . Less trivially, we have the following family.

## Theorem ([Smith, 2021c])

*Suppose  $g_\lambda(x)$  is irreducible. When  $j \in \mathbb{Z}$  is divisible by 256 and both  $\frac{j}{256}$  and  $\frac{j}{64} - 27 = \frac{1}{64}(j - 1728)$  are square-free, then  $\mathbb{Q}(\lambda) = \mathbb{Q}(E_\lambda[2])$  is monogenic over  $\mathbb{Q}$  with  $\lambda$  generating a power integral basis for the ring of integers.*

# Results for Division Fields of Elliptic Curves

---

# Main Result A

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

**Algorithm/theorem statement for  $p = 2$  [Smith, 2021c, Thm. 4.4]**

*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*

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

*is surjective. Then  $\mathbb{Q}(E[n])$  is not monogenic. Moreover, 2 is a common index divisor of  $\mathbb{Q}(E[n])$ .*

# Results for $p = 2$

$a_2$	$\sigma_2$	non-monogenic $n$
0	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	3, 5, 9, 11, 15, 17, 21, 27, 33, 43, 51, 57, 63, 85, 91, 93, 105, 117, 129, 171, 195, 255, 257, 273, 315, 331, 341, 381, 455, 513, 585, 657, 683, 771, 819, 993
1	$\begin{bmatrix} 1 & 1 \\ -2 & 0 \end{bmatrix}$	11
-1	$\begin{bmatrix} 0 & 1 \\ -2 & -1 \end{bmatrix}$	11, 23
2	$\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$	5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819
-2	$\begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}$	5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819

# Main Result B

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

**Theorem (Cor. 4.8 of [Smith, 2021c])**

*Let  $E/\mathbb{Q}$  be an elliptic curve without CM, then for infinitely many  $n > 1$  the division field  $\mathbb{Q}(E[n])$  is not monogenic.*

## Results for Abelian Varieties of Dimension $> 1$

---

## ...Or How to Sound Like You Understood a Talk

If you do something for elliptic curves, you can always ask the question, “Can I do this for abelian varieties?”

The construction of the Frobenius in [Duke and Tóth, 2002] was very important for our work with elliptic curves. They use Deuring lifting for their construction. For an arbitrary abelian variety such a canonical lift does not necessarily exist. Canonical lifts exist if we restrict to ordinary or almost ordinary abelian varieties, but we are interested in low  $p$ -rank too.



Instead, we opted to generalize the approach taken by [Centeleghe, 2016]. This approach relies on the fact that if  $A$  is an abelian variety over a field  $k$  with CM by a Gorenstein ring (i.e., if  $\text{End}_k(A)$  is a Gorenstein ring), then the Tate module  $T_\ell(A)$  is free of rank one over  $\text{End}_k(A) \otimes \mathbb{Z}_\ell$ . This is great! Now we **just** need to write down a basis for the relevant orders in an arbitrary CM field of degree  $2g$ , where the dimension  $g$  is greater than 1. Even if we restrict to  $g = 2$  and to maximal orders, this last step is difficult and results in an overwhelming number of cases. Thus we focus on the minimal case.

# The Minimal Endomorphism Ring

Suppose  $|k| = p^m = q$ .  $\text{End}_k(A)$  must contain **Frobenius**  $\pi$  and its dual **verschiebung**  $\nu$ . In fact, all orders of  $\text{End}_k(A) \otimes \mathbb{Q}$  containing  $\pi$  and  $\nu$  are endomorphism rings. Thus the smallest possible endomorphism ring is  $\mathbb{Z}[\pi, \nu]$ .

The characteristic polynomial of  $\pi$  is a *Weil  $q$ -polynomial*. We restrict to abelian varieties with irreducible Weil  $q$ -polynomials so that  $\mathbb{Z}[\pi, \nu]$  is Gorenstein.

# The Matrix Representing Frobenius

Let  $A/k$  be an abelian variety with an irreducible Weil  $q$ -polynomial and  $\text{End}_k(A) \cong \mathbb{Z}[\pi, \nu]$ . First, note that  $\{1, \pi, \dots, \pi^g, \nu, \dots, \nu^{g-1}\}$  forms a  $\mathbb{Z}$ -basis for  $\mathbb{Z}[\pi, \nu]$ .

Write

$$f(x) = x^{2g} + a_{2g-1}x^{2g-1} + \dots + a_1x + a_0$$

for the Weil  $q$ -polynomial of  $A$ . The following matrix yields the action of  $\pi$  on  $\mathbb{Z}[\pi, \nu]$ , and hence on  $T_\ell(A)$ .

# The Matrix Representing Frobenius

$$\sigma_p = \begin{matrix} & \begin{matrix} 1 & \pi & \pi^2 & \pi^{g-2} & \pi^{g-1} & \pi^g & v & v^2 & v^3 & & v^{g-1} \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & -qa_{g+1} & q & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 & -a_g & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & -a_{g+1} & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \dots & \vdots & -a_{g+i-1} & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 1 & 0 & -a_{2g-2} & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & -a_{2g-1} & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & -qa_2 & 0 & q & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & -qa_3 & 0 & 0 & q & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & -qa_{i+1} & \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & \dots & 0 & 0 & -qa_{g-1} & 0 & 0 & 0 & \dots & q \\ 0 & 0 & \dots & 0 & 0 & -q & 0 & 0 & 0 & \dots & 0 \end{bmatrix} & \begin{matrix} 1 \\ \pi \\ \pi^2 \\ \pi^i \\ \pi^{g-1} \\ \pi^g \\ v \\ v^2 \\ v^i \\ v^{g-2} \\ v^{g-1} \end{matrix} \end{matrix}$$

# Non-monogenic Division Fields of Abelian Surfaces

**Algorithm/theorem statement for  $p = 2$**  ([Smith, 2021a])

*Let  $A/\mathbb{F}_2$  be an abelian surface and write the Weil 2-polynomial of  $A$  as*

$$x^4 + a_3x^3 + a_2x^2 + 2a_3x + 2^2.$$

*Suppose the Weil 2-polynomial is irreducible,  $\text{End}_{\mathbb{F}_2}(A)$  is minimal, and*

$$\rho_{\hat{A},n} : \text{Gal}(\mathbb{Q}(\hat{A}[n])/\mathbb{Q}) \rightarrow \text{GSp}_4(\mathbb{Z}/n\mathbb{Z})$$

*is surjective for some  $\hat{A}/\mathbb{Q}$  that reduces to  $A$  modulo 2. Then Table 1 shows the odd  $n < 500$  for which the prime 2 is a common index divisor of  $\mathbb{Q}(\hat{A}[n])$  over  $\mathbb{Q}$ .*

# Non-monogenic Division Fields of Abelian Surfaces

$a_3$	$a_2$	$p$ -rank	non-monogenic $n$
-3	5	2	3, 19, 31, 57, 61, 93, 171, 183
-2	2	0	5, 7, 9, 13, 15, 21, 35, 37, 39, 45, 51, 61, 63, 65, 85, 91, 105, 109, 111, 117, 119, 133, 135, 153, 171, 185, 189, 195, 205, 219, 221, 241, 247, 255, 259, 273, 285, 305, 315, 325, 327, 333, 351, 357, 365, 377, 399, 455, 481, 485
-2	3	2	7, 47
-1	-1	2	5, 9, 11, 15, 23, 37, 43, 45, 67, 111, 127, 135, 151, 185, 203, 301, 333
-1	0	1	47
-1	1	2	3, 9, 103, 127
-1	3	2	5, 15, 59
0	-3	2	3, 5, 9, 11, 15, 23, 29, 33, 37, 45, 53, 87, 111, 135, 137, 185, 203, 233, 281, 301, 333
0	-2	0	3, 5, 7, 9, 11, 13, 15, 19, 21, 27, 33, 35, 39, 43, 45, 51, 57, 63, 65, 67, 73, 77, 81, 85, 91, 93, 99, 105, 109, 111, 117, 119, 129, 133, 135, 151, 153, 171, 185, 189, 195, 201, 217, 219, 221, 231, 241, 247, 255, 259, 273, 279, 285, 301, 315, 327, 331, 333, 337, 341, 351, 357, 365, 381, 387, 399, 441, 453, 455, 481, 485

**Table 1:** Odd  $n < 500$  where 2 is a common index divisor in  $\mathbb{Q}(\hat{A}[n])$

# Non-monogenic Division Fields of Abelian Surfaces

$a_3$	$a_2$	$p$ -rank	non-monogenic $n$
0	-1	2	3, 17, 19, 23, 31, 57, 61, 93, 171, 183, 229
0	1	2	3, 9, 17, 19, 23, 47, 57, 61, 69, 93, 171, 183, 229
0	2	0	3, 5, 7, 9, 13, 15, 19, 21, 27, 31, 35, 39, 45, 49, 51, 57, 63, 65, 73, 77, 85, 89, 91, 93, 99, 105, 109, 111, 117, 119, 127, 133, 135, 151, 153, 161, 171, 185, 189, 195, 217, 219, 221, 231, 241, 247, 255, 259, 273, 279, 285, 301, 315, 327, 331, 333, 337, 341, 351, 357, 365, 381, 387, 399, 441, 453, 455, 481, 485
1	-1	2	5, 7, 9, 11, 15, 37, 43, 45, 67, 79, 111, 135, 185, 203, 301, 333
1	0	1	47
1	1	2	3, 9
1	3	2	5, 15, 59
2	2	0	5, 7, 9, 13, 15, 21, 35, 37, 39, 45, 51, 61, 63, 65, 85, 91, 105, 109, 111, 117, 119, 133, 135, 153, 171, 185, 189, 195, 205, 219, 221, 241, 247, 255, 259, 273, 285, 305, 315, 325, 327, 333, 351, 357, 365, 377, 399, 455, 481, 485
2	3	2	7, 47
3	5	2	3, 19, 31, 57, 61, 93, 171, 183

**Table 2:** Odd  $n < 500$  where 2 is a common index divisor in  $\mathbb{Q}(\hat{A}[n])$

# Non-monogenic Division Fields of Abelian Varieties

**General Algorithm** ([Smith, 2021a]) *Let  $A/\mathbb{F}_p$  be an abelian variety and write the Weil  $p$ -polynomial of  $A$  as*

$$x^{2g} + a_{2g-1}x^{2g-1} + \cdots + p^{g-1}a_{2g-1}x + p^g.$$

*Suppose the Weil  $p$ -polynomial is irreducible,  $\text{End}_{\mathbb{F}_p}(A)$  is minimal, and*

$$\rho_{\hat{A},n} : \text{Gal}(\mathbb{Q}(\hat{A}[n])/\mathbb{Q}) \rightarrow \text{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$$

*is surjective for some  $\hat{A}/\mathbb{Q}$  that reduces to  $A$  modulo  $p$ . If  $\gcd(n, p) = 1$ , then  $n$  satisfies (5) if and only if  $p$  is a common index divisor of  $\mathbb{Q}(\hat{A}[n])/\mathbb{Q}$ .*

$$\prod_{\ell|n, \ell \text{ prime}} \left( (\ell - 1)\ell^{g^2} \prod_{i=1}^g (\ell^{2i} - 1) \right) \cdot (\ell^{2g^2+g+1})^{v_\ell(n)-1} > \sum_{d|\text{ord}_n(\sigma_p)} p^d \mu\left(\frac{\text{ord}_n(\sigma_p)}{d}\right). \quad (5)$$



# Non-monogenic Division Fields of Abelian Threefolds ( $p = 2$ )

$a_5$	$a_4$	$a_3$	$p$ -rank	non-monogenic $n$	$a_5$	$a_4$	$a_3$	$p$ -rank	non-monogenic $n$
-4	9	-15	3	7, 11, 23, 29, 43, 71, 87, 113, 127	0	1	-3	3	3, 9
-3	2	1	3	7, 11, 29, 43, 71, 87, 113, 127	0	1	-1	3	
-3	6	-9	3	3, 9, 27, 153	0	1	3	3	3, 9
-2	0	3	3	107, 149	0	2	-2	0	
-2	1	0	2	3, 5, 11, 55, 83	0	2	-1	3	7
-2	3	-5	3	3, 9, 27, 59, 63	1	-1	-5	3	3, 9
-2	3	-3	3	5, 83, 131	1	-1	-4	2	3, 7, 49
-2	5	-7	3	3, 7	1	0	-3	3	7, 77, 103
-1	-1	5	3	3, 9	1	0	1	3	3
-1	0	-1	3	3	1	1	0	2	3, 7
0	0	-3	3	3, 7, 9, 13, 15, 21, 27, 29, 31, 35, 39, 45, 63, 65, 87, 91, 93, 105, 117, 123, 141, 151, 195	2	4	6	0	3
0	0	-2	0	3, 7, 11, 15, 23, 29, 37, 45, 67, 71, 79	2	5	7	3	3, 7
0	0	-1	3	3, 5, 7, 15, 19, 21, 25, 35, 45, 63, 71, 75, 95, 97, 105, 123, 133	3	2	-1	3	7, 11, 23, 29, 43, 71, 87, 113, 127
0	0	1	3	3, 5, 7, 15, 19, 21, 25, 35, 45, 47, 49, 63, 75, 95, 97, 105, 123, 133	3	5	7	3	7
0	0	2	0	3, 7, 11, 15, 23, 29, 37, 45, 67	3	6	9	3	3, 9, 27, 153
0	0	3	3	3, 7, 9, 13, 15, 21, 27, 29, 31, 35, 39, 45, 47, 63, 65, 71, 87, 91, 93, 105, 117, 123, 141, 151, 195	4	9	15	3	7, 11, 29, 43, 71, 87, 113, 127

# Thank You!





Centeleghe, T. G. (2016).

**Integral Tate modules and splitting of primes in torsion fields of elliptic curves.**

*Int. J. Number Theory*, 12(1):237–248.



Duke, W. and Tóth, A. (2002).

**The splitting of primes in division fields of elliptic curves.**

*Experiment. Math.*, 11(4):555–565 (2003).



Gassert, T. A. (2017).

**A note on the monogeneity of power maps.**

*Albanian J. Math.*, 11(1):3–12.



Gras, M.-N. (1986).

**Non monogénéité de l'anneau des entiers des extensions cycliques de  $\mathbb{Q}$  de degré premier  $l \geq 5$ .**

*J. Number Theory*, 23(3):347–353.



Hensel, K. (1894).

**Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung.**

*J. Reine Angew. Math.*, 113:128–160.



Jakhar, A., Khanduja, S. K., and Sangwan, N. (2017).

**Characterization of primes dividing the index of a trinomial.**

*Int. J. Number Theory*, 13(10):2505–2514.



Narkiewicz, W. (2004).

**Elementary and analytic theory of algebraic numbers.**

Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition.



Neukirch, J. (1999).

**Algebraic number theory, volume 322 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].**

Springer-Verlag, Berlin.

Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.



Smith, H. (2021a).

**Frobenius finds non-monogenic division fields of abelian varieties.**



Smith, H. (2021b).

**The monogeneity of radical extensions.**

*Acta Arith.*, 198(3):313–327.



Smith, H. (2021c).

**Non-monogenic division fields of elliptic curves.**

*J. Number Theory*, 228:174–187.



Westlund, J. (1910).

**On the fundamental number of the algebraic number-field  
 $k(\sqrt[p]{m})$ .**

*Trans. Amer. Math. Soc.*, 11(4):388–392.

# An Example with an Ordinary Elliptic Curve

Suppose  $E$  is an elliptic curve with  $a_2 = 1$ . The characteristic polynomial of Frobenius is  $x^2 - x + 2$  and this has discriminant  $-7$ . Letting  $\pi$  denote the Frobenius endomorphism of  $E$  over  $\mathbb{F}_2$ , we have  $\text{End}_{\mathbb{F}_2}(E) \cong \mathbb{Z}[\pi] = \mathcal{O}_{\mathbb{Q}(\pi)}$ .

Combining all this information, we see Duke and Tóth's matrix representing  $\pi$  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  $\sigma_2$  modulo  $n$  by  $\text{ord}(\sigma_2, n)$ . This is the residue class degree of 2 in  $\mathbb{Q}(E[n])$ .



# An Example with an Ordinary Elliptic Curve

Generically, we expect the degree of  $\mathbb{Q}(E[n])$  over  $\mathbb{Q}$  to be  $|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|$ . Thus 2 will split into  $\frac{|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\mathrm{ord}(\sigma_2, n)}$  primes in  $\mathbb{Q}(E[n])$ .

The number of irreducible polynomials of degree  $m$  in  $\mathbb{F}_p[x]$  is  $\frac{1}{m} \sum_{d|m} p^d \mu\left(\frac{m}{d}\right)$ . With Dedekind's factorization theorem in mind, we compare  $\frac{|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\mathrm{ord}(\sigma_2, n)}$  and  $\frac{1}{\mathrm{ord}(\sigma_2, n)} \sum_{d|\mathrm{ord}(\sigma_2, n)} 2^d \mu\left(\frac{\mathrm{ord}(\sigma_2, n)}{d}\right)$ .

If the number of irreducible polynomial of degree  $\mathrm{ord}(\sigma_2, n)$  in  $\mathbb{F}_2[x]$  is less than  $\frac{|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\mathrm{ord}(\sigma_2, n)}$ , then 2 must divide the index of any monogenic order in  $\mathcal{O}_{\mathbb{Q}(E[n])}$ . We find that  $\sigma_2$  has order 10 modulo 11, so that 2 splits into 1320 primes in  $\mathbb{Q}(E[11])$ . There are only 99 irreducible polynomials of degree 10 in  $\mathbb{F}_2[x]$ . Thus 2 is a common index divisor of  $\mathbb{Q}(E[11])$  over  $\mathbb{Q}$ .