The University of Arizona, Tucson
College of Science
Department of Mathematics

Deuring Correspondence and Public Key Cryptography

Written Comprehensive Examination

Gaurish Korpal

December 07, 2023

Abstract

This report is about the correspondence between the worlds of *supersingular* elliptic curves and *definite* quaternion algebras. We will use illustrated toy examples throughout this exposition, just like the articles [Urb17; MP19; Cos20] that sparked my interest in isogeny-based cryptography. Furthermore, the titles for the sections indicate the phrase "Lights, Camera, Action" used in cinematography as the traditional cue to a film crew at the beginning of a take. That is, we will shed some light on the *theoretical aspects* in §1, look at the correspondence through the lens of *algorithms* in §2, and finally act on this knowledge by constructing some *cryptographic protocols* in §3.

Contents

Notation

p	positive prime integer
q	prime power p^n, with $n \geq 1$
ℓ	prime integer different from p
φ	Euler totient function
ψ	Dedekind psi function
K	field[1], like $\mathbb{Q}, \mathbb{R}, \mathbb{F}_q$, $\mathbb{Q}_p$, etc.
$\overline{K}$	a fixed algebraic closure of K, like $\overline{\mathbb{Q}} \coloneqq \mathbb{A}, \overline{\mathbb{R}} \coloneqq \mathbb{C}, \overline{\mathbb{F}}_q = \bigcup_{d \geq 1} \mathbb{F}_{q^d}$ (direct limit[2]), $\overline{\mathbb{Q}}_p$, $\mathbb{C}_p$, etc.
R	a commutative ring with identity[3] 1, like $\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, etc.
k	residue field of a local ring R with maximal ideal $\mathfrak{m}$, $k \coloneqq R/\mathfrak{m}$
ϖ	uniformizer of a discrete valuation ring R, $\mathfrak{m} = \langle \varpi \rangle = \varpi R$
v	discrete valuation of a local field or[4] place of a global field
$\mathrm{Pl}(K)$	set of places of a global field K
K_v	the local field that is completion of a global field K with respect to $v \in \mathrm{Pl}(K)$, like $\mathbb{Q}_p$, $\mathbb{Q}_\infty = \mathbb{R}$, etc.
$\mathbb{A}^n_R$	affine space (of relative dimension n) over R; the set of prime ideals of $R[t_1, \ldots, t_n]$
$\mathbb{P}^n_R$	projective space (of relative dimension n) over R; the set of homogeneous prime ideals of a graded R-algebra $R[t_0, \ldots, t_n]$
E	elliptic curve
$\mathcal{O}_E$	privileged rational point of E
$E(K)$	the abelian group of K-rational points on E
$+_E$	the group operation (addition) in $E(K)$
$K(E)$	function field of E over K
$\Delta(E)$	discriminant of E
$j(E)$	j-invariant[5] of E
ϕ	an isogeny, $\phi : E_1 \to E_2$
$\widehat{\phi}$	dual isogeny, $\widehat{\phi} : E_2 \to E_1$ such that $\widehat{\phi} \circ \phi = [\deg(\phi)]$
$\mathrm{Hom}_K(E, E')$	group of isogenies $E \to E'$ over K
$\mathrm{End}_K(E)$	endomorphism ring of E over K; $\mathrm{Hom}_K(E, E)$
$\mathrm{Aut}_K(E)$	automorphism group of E, invertible elements of $\mathrm{End}_K(E)$
$\mathrm{End}^0_K(E)$	endomorphism algebra of E; $\mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Q}$
$[m]$	multiplication-by-m endomorphism of E
$E[m]$	m-torsion subgroup of $E(\overline{K})$
π_n	p^n-power Frobenius isogeny; $\pi_n : E \to E^{(n)}$
π_E	Frobenius endomorphism of E; π_n for E over $\mathbb{F}_{p^n}$
$\mathrm{tr}(\bullet)$	matrix trace; trace of a linear transformation

[1] In 1871 Richard Dedekind introduced, for a set of real or complex numbers that is closed under the four arithmetic operations, the German word Körper, which means "body" or "corpus" (to suggest an organically closed entity). The English term "field" was introduced by Eliakim Hastings Moore in 1893. Also see the Wikipedia page: `https://de.wikipedia.org/wiki/Körper_(Algebra)`. Moreover, most of the fields of interest to us are *perfect fields* [Hus04, §7.6, 8.1] [Sil09] [Sut22, Definition 3.21, 4.38, Theorem 3.22]

[2] Let $\left\{\mathbb{F}_{q^d} | d \in \mathbb{N}\right\}$ be a family of finite fields of characteristic p. Whenever m divides n, we have the inclusion homomorphism $\mathbb{F}_{q^m} \to \mathbb{F}_{q^n}$. This gives the direct limit $\varinjlim_d \mathbb{F}_{q^d} = \bigcup_{d \geq 1} \mathbb{F}_{q^d}$. For more details, see this discussion `https://math.stackexchange.com/a/3617922`

[3] Therefore, for any ring homormophism $f : R \to R'$, we explicitly require $f(1) = 1$ [Cla15, p. 9]. That is, ring homomorphisms preserve 1 and a subring of a ring has the same 1 [Voi21, p. 21].

[4] There is a bijection between *valuations* and *places* on a global field [KKS11, §6.2(a, b)] [Mar17, Corollary 1.3.2] [Voi21, Rem 14.4.3]. In particular, if $\mathfrak{p}$ is a finite place (nonzero prime ideal of the ring of integers) of a number field K, then $v : K^\times \to \mathbb{R}$ is the $\mathfrak{p}$-adic (exponential) valuation which is normalized by the condition $v(K^\times) = \mathbb{Z}$ (discrete valuation) [Neu99, pp. 120–121].

[5] Felix Klein is credited with the introduction of j-function and j-invariant, see `https://mathoverflow.net/q/330049/`. For its various definitions see [Cox22, §§10.B, 11.A, 14.A] and [Sai13, §2.1].

$\mathrm{Tr}_{\Diamond/K}(\bullet)$	algebra (left) trace for some finite dimensional K-algebra $\Diamond$; $\mathrm{Tr}_{\Diamond/K}(\alpha) = \mathrm{tr}(\lambda_\alpha) \in K$ for $\alpha \in \Diamond$ and a (left) multiplication K-linear map $\lambda_\alpha : \Diamond \to \Diamond$ given by $\lambda_\alpha(\beta) = \alpha\beta$
$\mathrm{trd}(\bullet)$	reduced trace; $\mathrm{trd}(\alpha) \coloneqq \alpha + \overline{\alpha}$, where $\overline{}$ is a standard involution
$\mathrm{nrd}(\bullet)$	reduced norm; $\mathrm{nrd}(\alpha) \coloneqq \alpha\overline{\alpha}$, where $\overline{}$ is a standard involution
$\mathrm{Nm}_{\Diamond/K}(\bullet)$	algebra (left) norm for some finite dimensional K-algebra $\Diamond$; $\mathrm{Nm}_{\Diamond/K}(\alpha) = \det(\lambda_\alpha) \in K$ for $\alpha \in \Diamond$ and a (left) multiplication K-linear map $\lambda_\alpha : \Diamond \to \Diamond$ given by $\lambda_\alpha(\beta) = \alpha\beta$
$\mathcal{M}_0(N)_\Box$	a functor that assigns to a scheme over $\Box = \mathbb{Z}, \mathbb{Q}$ or $\mathbb{F}_p$ a set of isomorphism classes of pairs (E, C) such that C is a cyclic subgroup of E of order N; we omit writing $\Box = \mathbb{Q}$, i.e. $\mathcal{M}_0(N) = \mathcal{M}_0(N)_\mathbb{Q}$
$Y_0(N)_\Box$	a coarse moduli scheme of $\mathcal{M}_0(N)_\Box$; with $\mathcal{M}_0(N)_{\mathbb{F}_p}$ defined in this way for $p \nmid N$.
$X_0(N)_\Box$	compactification of $Y_0(N)_\Box$
$g_0(N)$	genus of $X_0(N)$
$\mathcal{H}$	complex upper half plane
$\Phi_N(X, Y)$	modular polynomial; model of a curve birational to $X_0(N)(\mathbb{C})$
$\mathcal{M}_0(Mp)_{\mathbb{F}_p}$	a functor that assigns to a scheme over $\mathbb{F}_p$ a set of isomorphism classes of triples (E, C', C'') such that C' is a cyclic subgroup of E of order M and C'' is a cyclic subgroup of E of order p, with $p \nmid M$
$\mathcal{M}_0(M)^{ss}_{\mathbb{F}_p}$	subfunctor of $\mathcal{M}_0(M)_{\mathbb{F}_p}$, $p \nmid M$, that assigns to a scheme over $\mathbb{F}_p$ a set of isomorphism classes of pairs (E, C) such that E is a supersingular elliptic curve and C is a cyclic subgroup of E of order M
$\mathbf{M}_N$	supersingular module over $X_0(N)$; module of supersingular points of $X_0(M)_{\mathbb{F}_p}$ for $N = Mp$
$Y_0(Mp)_{\mathbb{F}_p}$	an appropriately defined fiber of $Y_0(Mp)_\mathbb{Z}$
$X_0(Mp)_{\mathbb{F}_p}$	a union of two copies of $X_0(M)_{\mathbb{F}_p}$
w_p	Atkin-Lehner involution on $X_0(Mp)_{\mathbb{F}_p}$
$X_0^+(p)$	the quotient $X_0(p)/w_p$
$g_0^+(p)$	genus of $X_0^+(p)$
$\mathbb{S}$	the set of 15 supersingular primes
$G_\ell(p)$	supersingular ℓ-isogeny graph in characteristic p
A	separable quadratic K-algebra; an associative ring with unity and a ring homomorphism from K to the center of A such that $A \otimes_K \overline{K} \cong \overline{K} \times \overline{K}$
B	quaternion K-algebra; 4-dimensional central simple K-algebra
$(A, b \mid K)$	quaternion algebra defined by $A \supseteq K$ and $b \in K^\times$
$[a, b \mid K)$	quaternion algebra defined by $a \in K$, $b \in K^\times$ with $\operatorname{char} K = 2$
$(a, b \mid K)$	quaternion algebra defined by $a, b \in K^\times$ with $\operatorname{char} K \neq 2$
$\mathbb{H}$	Hamilton quaternion algebra; $(\mathbb{C}, -1 \mid \mathbb{R}) = (-1, -1 \mid \mathbb{R})$
$\mathrm{Ram}(B)$	ramification set of a global quaternion algebra B
$\mathrm{disc}(B)$	discriminant of a global quaternion algebra B
$B_{p,\infty}$	quaternion algebra over $\mathbb{Q}$ ramified at p and ∞
O	quaternion order
$\mathrm{discrd}(O)$	reduced discriminant
I	quaternion fractional ideal
$O_{\mathsf{L}}(I)$	left order of a quaternion fractional ideal I; similarly define $O_{\mathsf{R}}(I)$
$\mathrm{Cls}_{\mathsf{L}}(O)$	left class set of a quaternion order O; similarly define $\mathrm{Cls}_{\mathsf{R}}(O)$
$\mathrm{Typ}(O)$	type set of a quaternion order O; set of orders isomorphic to O
$\mathrm{Gen}(O)$	genus of a quaternion order O; set of orders connected to O

$I(O, O')$	the connecting ideal of quaternion orders O, O'; invertible integral O, O'-ideal with the smallest norm
$\mathrm{lev}(O)$	level of an Eichler order O
$E[I]$	scheme-theoretic intersection of $\ker(\phi)$ for all $\phi \in I \subset \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$
ϕ_I	isogeny from E to $E/E[I]$
$I(H)$	kernel left $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$-ideal for $H \leq E(\overline{\mathbb{F}}_p)$
I_ϕ	$I(\ker(\phi))$
$\mathcal{S}_M$	category of cyclic M-isogenies for supersingular curves; $\mathcal{S} \coloneqq \mathcal{S}_1$
$\mathcal{I}_M$	category of left fractional O-ideals, for Eichler order O of level M; $\mathcal{I} \coloneqq \mathcal{I}_1$
$G_\ell(K)$	supersingular ℓ-isogeny graph over $K = \mathbb{F}_p, \mathbb{F}_{p^2}$, or $\overline{\mathbb{F}}_p$
P	prover of an interactive proof protocol
V	verifier of an interactive proof protocol
$\xleftarrow{\$}$	sample randomly
$\overset{?}{=}$	check value
$\{0,1\}^*$	binary string
$\mathcal{R}$	binary relation; $\mathcal{R} \subseteq \{0,1\}^* \times \{0,1\}^*$
$L_{\mathcal{R}}$	language defined by $\mathcal{R}$
G	key generation algorithm
S	simulator
H	cryptographic hash function
$\mathfrak{M}$	message space
$\mathfrak{A}$	commitment space
$\mathfrak{C}$	challenge space
$\mathfrak{R}$	response space
σ	signature
L	product of primes $\ell_1, \ldots, \ell_r$
$\mathcal{B}$	bound for smooth number

1 Lights

1.1 ℓ-isogeny graphs

1.1.1 Elliptic curves

An *elliptic curve* over a field K is a smooth projective curve E over K, isomorphic to a closed subvariety of $\mathbb{P}^2_K$ defined by a homogeneous polynomial[6] $f(u,v,w)$ of the form

$$f(u,v,w) = v^2w - u^3 + a_1uvw - a_2u^2w + a_3vw^2 - a_4uw^2 - a_6w^3 \tag{1}$$

with the privileged rational point $\mathcal{O}_E = (0:1:0)$ [Liu06, Definition 6.1.25]. An elliptic curve is geometrically connected, like any projective plane curve and is of (arithmetic and geometric) genus 1 [Liu06, Corollary 7.4.5]. To ease notation, we generally write the affine equation for our elliptic curve using non-homogeneous coordinates $x = u/w$ and $y = v/w$,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

while always remembering that there is an extra point $\mathcal{O}_E = (0:1:0)$ out at infinity [Sil09, Proposition III.3.1]. For example, the smooth curve $x^3 + y^3 = 1$ over $\mathbb{Q}$ is an elliptic curve because it is isomorphic to $y^2 = x^3 - 432$ [Con99, Corollary 1.4.2][Sil93].

Let's visualize the elliptic curve[7] $E : y^2 = x^3 + x$ over different fields using SageMath [Ste12, §10.1] [Ara07, §2].

$K = \mathbb{Q}$

```
sage: E = EllipticCurve([0,0,0,1,0])
sage: E
Elliptic Curve defined by y^2 = x^3 + x over Rational Field
sage: plot(E) #over real numbers instead of rationals
Graphics object consisting of 1 graphics primitive
```

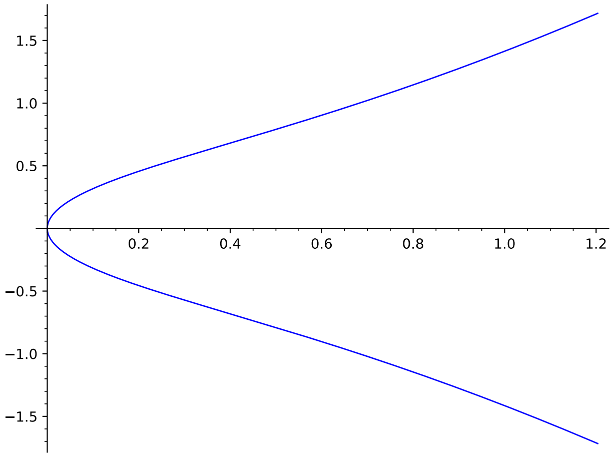


Figure 1: Not an ellipse! [RB12]

Note that even though $\mathbb{Q}$ is dense in $\mathbb{R}$, the above plot should only have one $\mathbb{Q}$-rational point.

[6] This is called *Weierstrass equation*, and the notation was first set up systematically by John Tate [Del75]. Also see the discussions on Math.SE: `https://math.stackexchange.com/q/743473` and `https://math.stackexchange.com/q/124732`

[7] Here $f(x,y) = y^2 - x^3 - x$ defines an elliptic curve because it is smooth, i.e. discriminant $\Delta(E) = -16(4(1)^3 + 27(0)^2) \neq 0$ [Sil09, Proposition III.1.4(a)].

$K = \mathbb{C}$

```
sage: #credit:RJ,https://www.math.wustl.edu/~acuna/content/Elliptic%20curves.html
sage: #the goal is to visualize the curve in C^2 = R^4
sage: #sage.schemes.riemann_surfaces.riemann_surface.RiemannSurface.plot_paths3d
sage: #here we use the parameterization done by Weierstrass P-function
sage: wp = E.weierstrass_p(prec=300).truncate(300) #Weierstrass P-function
sage: wpp = wp.derivative()/2 #(wpp)^2 = (wp)^3 - A*wp - B
sage: #take the real, and imaginary parts of wp as the first two coordinates,
sage: x = lambda u,v: wp(u+i*v).real()
sage: y = lambda u,v: wp(u+i*v).imag()
sage: #take the real part of wpp as the third coordinate
sage: z = lambda u,v: wpp(u+i*v).real()
sage: #use the imaginary part w of wpp to color the surface
sage: #use only the decimal part of w because the matplotlib
sage: #Python library selects colors from the colormap a number
sage: #between 0 and 1.
sage: w = lambda u,v: wpp(u+i*v).imag()
sage: cf = lambda u,v: w(u,v) - floor(w(u,v))
sage: cm = colormaps.hsv
sage: parametric_plot3d([x,y,z], (-2,2),(-2,2), aspect_ratio=1,color=(cf,cm)).
    add_condition(lambda x, y, z:  x^2+y^2+z^2 < 2^2).show(frame=false, viewpoint
    =[[0.5407,-0.5759,-0.6132],239.87]) #did manual adjustments of viewpoint
None
```

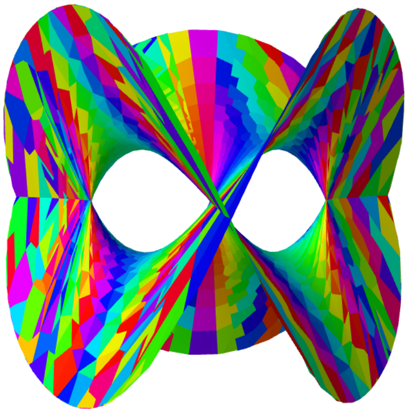


Figure 2: Curve is surface! [NG22]

Elliptic curve over $\mathbb{C}$ can be seen as an embedding of a torus in the complex projective plane [BD16]. Moreover, by unfolding the above knotted surface, we can obtain the torus [BA19].

$K = \mathbb{F}_{23}$

```
sage: E0 = EllipticCurve(GF(23), [0,0,0,1,0])
sage: E0
Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size 23
sage: E0.plot(pointsize=50, gridlines=True) #for field ext use E0.points()
Graphics object consisting of 1 graphics primitive
```

In fact, deep analogies exist between finite-field theoretic and complex-analytic properties of equations. For instance, the line between two points of the elliptic curve over finite field wraps around at the borders, just like torus [Sul13; Ken20].

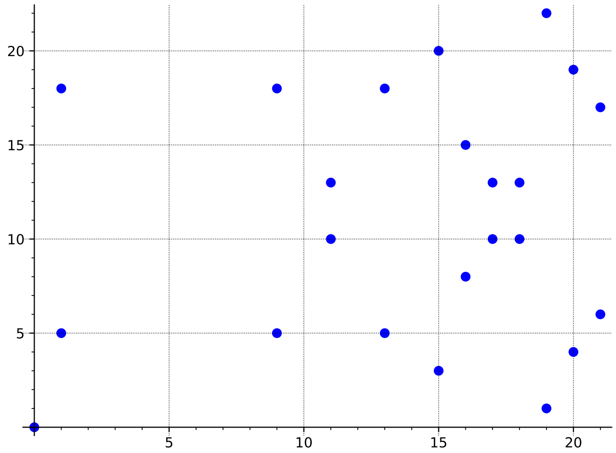


Figure 3: A "smooth" curve over $\mathbb{F}_{23}$! [Kob82]

Note that the above three plots are of the affine equation, and do not include the privileged point $\mathcal{O}_E$, which lies at infinity. For a projective view of these affine sketches see [Ken21].

The fact that the rational points $E(K)$ on elliptic curves E/K form an abelian group with identity element $\mathcal{O}_E$ was first pointed out by Christian Juel in 1896 [Lem11a]. This group is determined by the condition that three points sum to the zero element $\mathcal{O}_E$ if and only if they lie on a common line in the projective plane [Ste12, §10.1.1] [Sut22, §2.1 & 2.2] [Gal12, §7.9] [Mor91, §5.6.3]. Moreover, elliptic curves are one-dimensional abelian[8] varieties, i.e., a "nice" projective group variety over K [Sut22, §2.3][Liu06, Proposition 10.2.9]. Concretely, we know the following about the structure of this group:

$$E(\mathbb{C}) \cong \mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z} \tag{3}$$

$$E(\mathbb{R}) \cong \begin{cases} \mathbb{R}/\mathbb{Z} & \text{if } \Delta(E) < 0 \\ \mathbb{R}/\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } \Delta(E) > 0 \end{cases} \tag{4}$$

$$E(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}^r \oplus \mathbb{Z}/m\mathbb{Z} & \text{for } m = 1, 2, \ldots, 9, 10, 12 \\ \mathbb{Z}^r \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} & \text{for } m = 2, 4, 6, 8 \end{cases} \qquad \text{with } r \geq 0 \tag{5}$$

$$E(\mathbb{F}_q) \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \qquad \text{with } m_1 | m_2 \text{ and } m_1 | q-1 \tag{6}$$

where (3) and (4) follow from uniformization theorem of Poincaré (1901) [Sil09, Corollary VI.5.1.1] [Sil94, Corollary V.2.3.1] [Sut22, Problem 8.3]; (5) follows[9] from the theorems of Mordell (1922) and Mazur (1977) [Sil09, Theorem VIII.4.1] [Dar09, Theorem 3.14] [SZ03, §6.5] [Loz11, §2.4]; and (6) follows from the theorem of Rück (1987) [Men93, §2.6 & 5.4] [Eng99, Theorem 3.76] [Was08, Theorem 4.1] [Gal12, Theorem 9.8.2] [Sut22, Corollary 6.4] [Sil09, Exercise 5.6]. Moreover, for instance, if $E : y^2 = x^3 + x$ is an elliptic curve over $K = \mathbb{Q}$ or $K = \mathbb{F}_{23}$ then we can use SageMath to determine the structure of $E(K)$:

```
sage: E.torsion_subgroup()
Torsion Subgroup isomorphic to Z/2 associated to the Elliptic Curve defined by y
    ^2 = x^3 + x over Rational Field
sage: E.rank()
0
sage: E0.abelian_group()
```

[8] An abelian variety over K is defined to be an algebraic group that is geometrically integral and proper over K [Liu06, Definition 7.4.37]. A complex abelian variety is a smooth projective variety which happens to be a complex torus. Abelian varieties are indeed abelian groups (unlike elliptic curves which aren't ellipses), however the use "abelian" here comes about from the connection with abelian integrals which generalize elliptic integrals [Ara12].

[9] The proof of the possible torsion subgroups involves modular curves, discussed in §1.1.2, see [Maz77] [Maz78]. However, the rank r is inaccessible by elementary methods. Moreover, in 1965, Birch and Swinnerton-Dyer conjectured that the rank r is the order of the zero of the Hasse–Weil L-function $L(E, s)$ at $s = 1$ [Dar04].

```
Additive abelian group isomorphic to Z/24 embedded in Abelian group of points on
    Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size 23
```

Furthermore, the structure-preserving maps between elliptic curves (and more generally, abelian varieties) are called *isogenies*. The term "isogeny" was introduced by André Weil, where the word isogeny literally means "equal origins". The Greek prefix "iso" means equal and the Greek root "gene" means origin (as in the word genesis) [Sut22, §4]. That is, if E_1 and E_2 are elliptic curves over K then an isogeny over K is defined[10] as a morphism[11] $\phi : E_1 \to E_2$ of varieties over K such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ [Sil09, §III.4][Gal12, §9.6 & 25.1][Eng99, §3.1 & 5.4]. Furthermore, if there exist isogenies $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_1$ whose compositions are the identity morphisms, then ϕ_1 and ϕ_2 are called *isomorphisms* [Sut22, Definition 4.22].

An important example of an isogeny[12] is the *multiplication-by-m* map defined as:

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto \begin{cases} \underbrace{P +_E P +_E \cdots +_E P}_{m \text{ times}} & \text{if } m > 0 \\ \mathcal{O}_E & \text{if } m = 0 \\ [-m](-P) & \text{if } m < 0 \end{cases} \end{aligned}$$

Concretely, for any point $P = (x, y)$ on an elliptic curve given by (2), we have

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

where $\psi_m \in K[x,y]$ is called the mth division polynomial of E and $\theta_m, \omega_m \in K[x,y]$ can be expressed in terms of sequence ψ_m [Sil09, Example III.4.1 & Exercise 3.7][BSS00, §III.4][Sut22, §5.6]. Moreover, there exists many efficient point multiplication algorithms [BSS00, §IV.2]. For example, for $E : y^2 = x^3 + x$ we can use SageMath to evaluate multiplication-by-23 map over $K = \mathbb{Q}$ and $K = \mathbb{F}_{23}$:

```
sage: phi = E.scalar_multiplication(23) #alter: E.multiplication_by_m_isogeny(23)
sage: phi
Scalar-multiplication endomorphism [23] of Elliptic Curve defined by y^2 = x^3 +
    x over Rational Field
sage: P = E(0,0) #P=(0:0:1) is the only non-trivial rational point, [2]P = \mo_E
sage: phi(P)
(0 : 0 : 1)
sage: phi0 = E0.scalar_multiplication(23)
sage: phi0
Scalar-multiplication endomorphism [23] of Elliptic Curve defined by y^2 = x^3 +
    x over Finite Field of size 23
sage: P0 = E0(15,20) #P_0=(15:20:1) taken from the plot above
sage: phi0(P0)
(15 : 3 : 1)
```

The *degree* of a non-zero isogeny $\phi : E_1 \to E_2$ is the degree of the morphism, i.e. $\deg(\phi) = [K(E_1) : \phi^* K(E_2)] < \infty$ with $\phi^* : K(E_2) \to K(E_1)$ defined as $\phi^* f = f \circ \phi$ [Sil09, §II.2, III.4] [Gal12, Definition 8.1.6, 9.6.1, Lemma 9.6.13] [Sut22, Remark 4.32]. The degree of the zero isogeny (constant morphism) is defined to be 0. If there is a non-zero isogeny (respectively, isogeny of degree $d > 0$) between two elliptic curves E_1 and E_2 then we say that E_1 and E_2 are *isogenous*[13] (respectively, *d-isogenous*). In particular, 1-isogenous

[10] Under this definition, the zero morphism, which maps every point on $E_1(\overline{K})$ to $\mathcal{O}_{E_2}$, is an isogeny. However, in the case of elliptic curves, this convention is not always followed, for example see [Sut22, §4.2] [Was08, §12.2] [Hus04, §12.3] [De +20, §2.1] [Voi21, Definition 42.1.2]. Moreover, the standard convention for general group varieties requires isogenies to preserve dimension, i.e. they must be surjective and have finite kernel.

[11] Let X and Y be varieties over K and let $U \subset X$ be open. A rational map $\phi : U \to Y$ over K which is regular at every point $P \in U(K)$ is called a *morphism* over K [Sil09, §I.3] [Gal12, §5.5].

[12] This is also called an *endomorphism* because it is a morphism from a mathematical object to itself. An endomorphism that is also an isomorphism is an *automorphism* [Sil09, §III.10].

[13] Tate's isogeny theorem states that any two elliptic curves over $\mathbb{F}_q$ have the same number of points iff they are isogenous over $\mathbb{F}_q$ [Tat66, Theorem 1(c)] [Hus04, Theorem 13.8.4] [Gal12, Theorem 9.7.4, Lemma 9.11.13] [Cox22, Proposition 14.19].

elliptic curves are said to *isomorphic* and belong to the same *isomorphism class* [Sil09, Corollary II.2.4.1] [Gal12, Lemma 8.1.13, 8.1.15]. In fact, if E_1, E_2 are isomorphic then $j(E_1) = j(E_2)$. The converse is also true if K is an algebraically closed field, i.e. there exists an isomorphism from E_1 to E_2 defined over $\overline{K}$ iff $j(E_1) = j(E_2)$ [Sil09, Proposition III.1.4(b)] [Sut22, §13.2]. Moreover, if $K = \mathbb{F}_q$ then the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$, denoted by N_q, is given by

$$N_q = 2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right) \tag{7}$$

where $\left(\frac{\bullet}{*}\right)$ denotes the Kronecker symbol [Men93, Theorem 3.1].

```
sage: (2*23) + 3 + kronecker(-4,23) + 2*kronecker(-3,23) #the number of isomorphism classes of elliptic curves over F_23
46
sage: E0.j_invariant()
3
sage: from sage.schemes.elliptic_curves.ell_finite_field import curves_with_j_1728
sage: curves_with_j_1728(GF(23)) #pairwise non-isomorphic elliptic curves with j-invariant 1728 over F_23; Also see [Gal12, Exercise 9.11.14]
[Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size 23, Elliptic Curve defined by y^2 = x^3 + 22*x over Finite Field of size 23]
sage: E0 == curves_with_j_1728(GF(23))[0]
True
sage: E1 = curves_with_j_1728(GF(23))[1]
sage: E0.change_ring(GF(23^2)).is_isomorphic(E1.change_ring(GF(23^2)))
True
```

Surprisingly, if $\phi : E_1 \to E_2$ is a non-constant isogeny of degree m then there exists a unique isogeny[14] $\hat{\phi} : E_2 \to E_1$, called *dual isogeny*, satisfying $\hat{\phi} \circ \phi = [m]$ [Sil09, Theorem III.6.1(a)]. If $\phi = [0]$, then we set $\hat{\phi} = [0]$. Therefore, $\widehat{[m]} = [m]$ and $\deg([m]) = m^2$ [Sil09, Theorem III.6.2(d)]. For example, we can use SageMath to verify this for the multiplication-by-23 maps over $K = \mathbb{Q}$ and $K = \mathbb{F}_{23}$:

```
sage: phi.dual() is phi
True
sage: phi.degree() == 23^2
True
sage: phi0.dual() is phi0
True
sage: phi0.degree() == 23^2
True
```

If L is a field such that $\phi^*(K(E_2)) \subset L \subset K(E_1)$ and $K(E_1)/L$ is separable and $L/\phi^*(K(E_2))$ is purely inseparable field extension[15], then the *separable degree* of ϕ is $\deg_s(\phi) = [K(E_1) : L]$ and the *inseparable degree* of ϕ is $\deg_i(\phi) = [L : \phi^*(K(E_2))]$. Furthermore, a non-zero isogeny is called *separable* (respectively, *inseparable*) if its inseparable (respectively, separable) degree is 1 [Gal12, Definition 8.1.6]. That is, over a field of characteristic zero, every non-zero isogeny is separable [Sut22, Corollary 5.2]. Moreover, isomorphisms are both seprable and inseparable [Sut22, Remark 5.7]. For example, we can use SageMath to check this for the multiplication-by-23 maps over $K = \mathbb{Q}$ and $K = \mathbb{F}_{23}$:

```
sage: phi.is_separable()
True
sage: phi0.is_separable()
```

[14] Recall that an isomorphism ϕ of elliptic curves is an invertible isogeny, equivalently, an isogeny of degree 1. That is, if ϕ is an isomorphism then the dual isogeny gives an inverse isomorphism, since $\hat{\phi} \circ \phi = \phi \circ \hat{\phi} = [1] = \mathrm{id}_E$.

[15] An element α, algebraic over a field K', is separable (respectively, purely inseparable) if the minimal polynomial of α over K has distinct roots (respectively, one root) in K'. An algebraic field extension L'/K' is called a *separable* extension if every $\alpha \in L'$ is separable over K' [Gal12, §A.6].

```
False
```

In fact, if E is an elliptic curve over K and $m \in \mathbb{Z}$ then $[m]$ is separable if and only if m is coprime to the characteristic of K [Sil09, Corollary III.5.4] [Sut22, Theorem 5.25]. Moreover, if K has characteristic p, then $[p] = \widehat{\pi}_1 \circ \pi_1$, where π_1 belongs to the most important family of inseparable isogenies [Sil09, §V.3] [Sut22, §13.1]. The *p^n-power Frobenius isogeny*[16] π_n, $n \geq 1$, is defined for an elliptic curve E over a field K of characteristic p as

$$\pi_n : E \to E^{(p^n)}$$
$$(u : v : w) \mapsto (u^{p^n} : v^{p^n} : w^{p^n})$$

where $E^{(p^n)}$ is given by

$$f^{(p^n)}(u, v, w) = v^2 w - u^3 + a_1^{p^n} uvw - a_2^{p^n} u^2 w + a_3^{p^n} vw^2 - a_4^{p^n} uw^2 - a_6^{p^n} w^3$$

if E is given by (1). In particular, π_n is an inseparable isogeny of degree $q = p^n$ [Hus04, Definition 13.5.2] [Sil09, Proposition II.2.11]. For example, for $E : y^2 = x^3 + x$ we can use SageMath to evaluate π_4 over $K = \mathbb{F}_{23}$:

```
sage: pi4 = E0.frobenius_isogeny(4)
sage: pi4
Frobenius endomorphism of degree 279841 = 23^4:
  From: Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size 23
  To:   Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size 23
sage: pi4.rational_maps()
(x^279841, y^279841)
sage: pi4.is_separable()
False
```

For an elliptic curve E over $K = \mathbb{F}_q$ with $q = p^n$, we get *Frobenius endomorphism* $\pi_E := \pi_n : E \to E$ [Hus04, Definition 13.1.1] [Was08, §4.2] [Sil09, Example III.4.6]. It induces a group isomorphism from $E(\overline{\mathbb{F}}_q)$ to $E(\overline{\mathbb{F}}_q)$, since over the algebraic closure we can take qth roots of coordinates of points, and doing so still fixes elements of $\mathbb{F}_q$. However, as an isogeny, π_E is not an isomorphism because there is no rational map from $E \to E$ that acts as its inverse [Sut22, Remark 4.25] [Gal12, Example 9.6.14]. Furthermore, we define the *trace of Frobenius* π_E as $\operatorname{tr}(\pi_E) := q + 1 - \#E(\mathbb{F}_q)$ with $|\operatorname{tr}(\pi_E)| \leq 2\sqrt{q}$ [Hus04, Definition 12.4.2] [Sil09, Theorem III.9.3, Remark V.2.6] [Gal12, §9.10] [Sut22, Definition 6.17, Theorem 7.3]. For $t \in \mathbb{Z}$ such that $|t| \leq 2\sqrt{q}$ there exists an elliptic curve E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$ and $E(\mathbb{F}_q)$ cyclic [Hus04, Theorem 13.8.5] [Gal12, §9.10]. In fact, we can extend (7) to get $N_q(t)$, the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ corresponding to the value t for $t \in \mathbb{Z}$ with $|t| \leq 2\sqrt{q}$ [Men93, Theorem 3.2] [Eng99, Theorem 3.75]. The following are some computations we can do for $E : y^2 = x^3 + x$ over $K = \mathbb{F}_{23}$ using SageMath:

```
sage: piE = E0.frobenius_endomorphism() #this is pi_E
sage: piE == E0.frobenius_isogeny(1) #in this case pi_E = pi_1
True
sage: E0.trace_of_frobenius() #involves counting the number of points
0
sage: E0.frobenius_polynomial() #characteristic polynomial [Was08, Prop 4.11]
x^2 + 23
```

The *kernel* of an isogeny $\phi : E_1 \to E_2$ over K is the finite subgroup of $E_1(\overline{K})$ defined as $\ker(\phi) = \phi^{-1}(\mathcal{O}_{E_2}) := \{P \in E_1(\overline{K}) : \phi(P) = \mathcal{O}_{E_2}\}$ [Sil09, Corollary III.4.9] [Gal12, Definition 9.6.1]. Note that, since all cosets of a group have the same size, for all $Q \in E_2(\overline{K})$, $\#\phi^{-1}(Q) = \#\ker(\phi)$. In particular, $\#\ker(\phi) = \deg_s(\phi)$ [Sil09, Theorem III.4.10] [Gal12, Lemma 9.6.4] [Sut22, Theorem 5.8]. An isogeny $\phi : E_1 \to E_2$ is said to be *cyclic* if its kernel is a cyclic group. Moreover, if E is an elliptic curve over K and $H \subseteq E(\overline{K})$ is a finite group that is defined[17] over K then there is a unique (up to isomorphism over $\overline{K}$) elliptic curve $E' = E/H$

[16] The dual isogeny $\widehat{\pi}_n$ is called the Verschiebung [Gal12, Example 9.6.24].

[17] That is, $\tau(P) \in H$ for all $P \in H$ and $\tau \in \operatorname{Gal}(\overline{K}/K)$. Moreover, the condition of being defined over K can be ignored by taking a field extension.

over K and a (not necessarily unique) separable isogeny[18] $\phi : E \to E'$ over K such that $\ker(\phi) = H$ [Hus04, Remark 13.5.1] [Sil09, Theorem III.4.12, Exercise 3.13] [Gal12, Theorem 9.6.19, Exercise 9.6.20, Corollary 25.1.7] [Sut22, Theorem 5.11, 5.13, 5.15, Problem 3.2]. Thus two separable isogenies $\phi_1, \phi_2 : E \to E'$ are said to be *equivalent* if $\ker(\phi_1) = \ker(\phi_2)$ [Gal12, Exercise 25.1.1, Example 25.1.15, Remark 25.3.2]. For example, we can use SageMath to get a separable cyclic isogeny from $E : y^2 = x^3 + x$ over $K = \mathbb{F}_{23}$ with the the kernel generated by the point $P_0 = (15 : 20 : 1)$.

```
sage: P0.order() #we will use this point as the generator of kernel
8
sage: velu = EllipticCurveIsogeny(E0, P0) #cyclic isogeny using Velu's formula
sage: velu
Isogeny of degree 8 from Elliptic Curve defined by y^2 = x^3 + x over Finite
    Field of size 23 to Elliptic Curve defined by y^2 = x^3 + 15 over Finite Field
     of size 23
```

If $\phi : E_1 \to E_2$ is an isogeny between elliptic curves over a field of characteristic p then it factors as $E_1 \xrightarrow{\pi_n} E_1^{(p^n)} \xrightarrow{\tau} E_2$ where τ is a separable isogeny and π_n is the p^n-power Frobenius isogeny for $p^n = \deg_i(\phi)$ [Sil09, Corollary II.2.12] [Sut22, Corollary 5.4, Remark 5.5]. Furthermore, an isogeny can be written as a "chain" of prime-degree isogenies [Gal12, Theorem 25.1.2] [Sut22, Corollary 5.12] [Ler22, §1.1.2]. Moreover, since isogenies of prime degree are cyclic, we usually restrict our attention to cyclic isogenies [Sil09, Example IX.6.4] [Voi21, Remark 42.3.10] [Sut22, Definition 20.1] [Ler22, §1.1.2]. This observation is of crucial importance for the algorithms.

```
sage: from sage.schemes.elliptic_curves.hom_composite import
    EllipticCurveHom_composite
sage: chain = EllipticCurveHom_composite(E0, P0) #decomposing Velu's formula into
     prime steps is exponentially faster
sage: chain
Composite morphism of degree 8 = 2^3:
  From: Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size 23
  To:   Elliptic Curve defined by y^2 = x^3 + 15 over Finite Field of size 23
sage: chain.factors()
(Isogeny of degree 2 from Elliptic Curve defined by y^2 = x^3 + x over Finite
    Field of size 23 to Elliptic Curve defined by y^2 = x^3 + 19*x over Finite
    Field of size 23, Isogeny of degree 2 from Elliptic Curve defined by y^2 = x^3
     + 19*x over Finite Field of size 23 to Elliptic Curve defined by y^2 = x^3 +
    2*x + 3 over Finite Field of size 23, Isogeny of degree 2 from Elliptic Curve
    defined by y^2 = x^3 + 2*x + 3 over Finite Field of size 23 to Elliptic Curve
    defined by y^2 = x^3 + 15 over Finite Field of size 23)
sage: chain == velu
True
```

The kernel[19] of the multiplication-by-m map $[m] : E \to E$ is called the *m-torsion subgroup* of E, defined as $E[m] := \ker([m]) = \{P \in E(\overline{K}) : [m]P = \mathcal{O}_E\}$ [Eng99, Definition 3.8] [Gal12, Definition 9.1.2] [Sut22, §5]. The m-torsion subgroups play a key role in the theory of elliptic curves[20] [Was08, Chapter 3]. If $p \geq 0$ is the characteristic of K, then

$$E[m] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} & \text{if } m \neq 0 \text{ in K} \\ \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m'\mathbb{Z} \text{ or } \mathbb{Z}/m'\mathbb{Z} \oplus \mathbb{Z}/m'\mathbb{Z} & \text{if } m = p^n m', p > 0, p \nmid m', n \in \mathbb{Z}_{>0} \end{cases} \tag{8}$$

that is, $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank two when $m \neq 0$ [Hus04, Theorem 12.3.6] [Was08, Theorem

[18] Therefore, loosely speaking, every group homomorphism $E(K) \to E'(K)$ with finite kernel is an isogeny. However, since a non-zero isogeny has finite degree and hence finite kernel, not every group homomorphism is an isogeny. For example, if $E(\mathbb{Q}) \cong \mathbb{Z}$ and $E'(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ then we get a non-zero group homomorphism $E(\mathbb{Q}) \to E'(\mathbb{Q})$ whose kernel is infinite.

[19] Some authors, like [Sil09, §III.4, 6] define it as "the set of points of $E(\overline{K})$ of order m"

[20] For example, as noted above, $E(\overline{\mathbb{F}}_q)$ is a torsion group, i.e., for each point $P \in E(\overline{\mathbb{F}}_q)$ there is a positive integer m such that $[m]P = \mathcal{O}_E$ [Men93, Example 2.16, 2.17, 2.18]. Therefore, understanding the structure of $E[m]$ allows us to understand the structure of $E(\mathbb{F}_q)$ discussed above, and also turns out to be the key to efficiently computing $\#E(\mathbb{F}_q)$.

3.2] [Sil09, Corollary III.6.4, Proposition VI.6.1] [Sut22, Theorem 6.1]. Moreover, we can use SageMath to compute $E(\mathbb{F}_q)[m]$, the subgroup of m-torsion points[21] in $E(\mathbb{F}_q)$ i.e. $E[m] \cap E(\mathbb{F}_q)$, for $m > 0$. For example, consider $E : y^2 = x^3 + x$ over various extensions of $\mathbb{F}_{23}$:

```
sage: E0.abelian_group().torsion_subgroup(13)
Trivial group embedded in Abelian group of points on Elliptic Curve defined by y
    ^2 = x^3 + x over Finite Field of size 23
sage: E0.change_ring(GF(23^2)).abelian_group().torsion_subgroup(13)
Trivial group embedded in Abelian group of points on Elliptic Curve defined by y
    ^2 = x^3 + x over Finite Field in z2 of size 23^2
sage: E0.change_ring(GF(23^3)).abelian_group().torsion_subgroup(13)
Additive abelian group isomorphic to Z/13 embedded in Abelian group of points on
    Elliptic Curve defined by y^2 = x^3 + x over Finite Field in z3 of size 23^3
sage: E0.change_ring(GF(23^4)).abelian_group().torsion_subgroup(13)
Trivial group embedded in Abelian group of points on Elliptic Curve defined by y
    ^2 = x^3 + x over Finite Field in z4 of size 23^4
```

If E is an elliptic curve defined over a field K of characteristic $p > 0$, then the possibilities for $E[p]$ being isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or $\{0\}$ admitted by (8) motivates the following definitions. If $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ then E is said to be *ordinary*, and if $E[p] \cong \{0\}$, we say that E is *supersingular*[22] [Hus04, Theorem 13.5.6] [TVN07, Proposition 2.4.18] [Was08, Theorem 3.2] [Sai14, Proposition 8.2] [Sut22, Definition 6.2.] [Ler22, Proposition 1.1.5]. In this report we will discuss various equivalent characterizations of supersingular elliptic curves [Hus04, Table 13.2]. For example, E is supersingular iff the multiplication-by-p map $[p] : E \to E$ is inseparable and $j(E) \in \mathbb{F}_{p^2}$ [Hus04, Theorem 13.5.6] [Sil09, Theorem V.3.1] [Sut22, Theorem 13.16]. Therefore, the property of being ordinary or supersingular is invariant under base change[23], and in any field K of positive characteristic, the number of $\overline{K}$-isomorphism classes of supersingular elliptic curves is finite (it certainly cannot exceed $\#\mathbb{F}_{p^2} = p^2$) [KM85, Theorem 2.9.4]. A supersingular elliptic curve is also said to have *Hasse invariant* 0, i.e., an elliptic curve E defined by a cubic equation (1) over a field K of characteristic p is supersingular iff the coefficient of $(uvw)^{p-1}$ in $f(u, v, w)^{p-1}$ is zero [Hus04, Definition 13.3.1, Proposition 3.5] [Sil09, Theorem V.4.1] [Sut22, Problem 4.1]. We can use SageMath to verify this for $E : y^2 = x^3 + x$ and its 8-isogenous curve $E' : y^2 = x^3 + 15$ over $\mathbb{F}_{23}$:

```
sage: E0.hasse_invariant()
0
sage: EllipticCurve(GF(23), [0,0,0,0,15]).hasse_invariant()
0
```

Therefore, both of these curves are supersingular. In fact, the property of being ordinary or supersingular is an isogeny invariant [Sut22, Theorem 13.2] [Sil09, Example V.4.5] [Was08, Proposition 4.33, 4.37]. Furthermore, we can determine the number of $\overline{K}$-isomorphism classes S_p of supersingular elliptic curves (with the representative curves are defined over $\mathbb{F}_{p^2}$)

$$S_p = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \pmod{12} \\ 1 & \text{if } p = 2, 3;\ p \equiv \pm 5 \pmod{12} \\ 2 & \text{if } p \equiv -1 \pmod{12} \end{cases} \tag{9}$$

where $E : y^2 + y = x^3$ and $E : y^2 = x^3 + x$ are the representatives for $p = 2$ and $p = 3$, respectively [Igu58] [DR73, §VI.4.9] [KM85, Cor 12.4.6] [Hus04, §13.4] [Was08, Cor 4.40] [Sil09, §V.4, Exercise 5.9] [Sai14, Example 8.6]. For example, $S_{23} = 1 + 2 = 3$ with the isomorphism classes represented by $E_1 : y^2 = x^3 + x$, $E_2 : y^2 = x^3 + 1$ and $E_3 : y^2 = x(x - 1)(x - 3)$ [Was08, Example 4.14] [Voi21, Example 42.3.12].

Now, if E is an elliptic curve defined over $K = \mathbb{F}_q$ then E is supersingular iff p divides $\mathrm{tr}(\pi_E)$ [Men93, Corollary 2.11] [Eng99, Corollary 3.73] [Was08, Proposition 4.31] [Sil09, Exercise 5.10] [Gal12, §9.11] [Sai14, Proposition 8.5] [Sut22, Theorem 13.3]. This property is used in SageMath to determine whether a given elliptic curve over a finite field is supersingular:

[21] Some authors call these *m-division points*, denoted by ${}_mE(\mathbb{F}_q)$ [Hus04, Definition 12.1.4].

[22] We will talk about the origin of this terminology in §1.3

[23] If E is an elliptic curve over K and L/K is any field extension, the separable degree of $[p]$ on E_L does not depend on L

```
sage: E0.is_supersingular()
True
sage: EllipticCurve(GF(23), [0,0,0,0,15]).is_supersingular()
True
```

This also lets us say more about the group structure of $E(\mathbb{F}_q)$ when E is supersingular

$$E(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{if } \operatorname{tr}(\pi_E) = \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q} \\ \mathbb{Z}/(\sqrt{q}-1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q}-1)\mathbb{Z} & \text{if } \operatorname{tr}(\pi_E) = 2\sqrt{q} \\ \mathbb{Z}/(\sqrt{q}+1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q}+1)\mathbb{Z} & \text{if } \operatorname{tr}(\pi_E) = -2\sqrt{q} \\ \mathbb{Z}/m\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/\left(\frac{q+1}{2}\right)\mathbb{Z} & \text{if } \operatorname{tr}(\pi_E) = 0 \end{cases} \tag{10}$$

where $m \in \mathbb{Z}_{\geq 1}$ [Men93, Lemma 2.13] [Eng99, Theorem 3.74] [SZ03, §3.3] [TVN07, Theorem 3.3.15] [Was08, Theorem 4.4] [Gal12, Theorem 9.10.13]. Recall that for $E : y^2 = x^3 + x$ over $\mathbb{F}_{23}$ we got $\operatorname{tr}(\pi_E) = 0$ and $E(\mathbb{F}_{23}) = \mathbb{Z}/24\mathbb{Z}$, which agrees with this result. We can also look at $E : y^2 = x^3 + x$ over $\mathbb{F}_{23^2}$ using SageMath:

```
sage: E0.change_ring(GF(23^2)).trace_of_frobenius()
-46
sage: E0.change_ring(GF(23^2)).abelian_group()
Additive abelian group isomorphic to Z/24 + Z/24 embedded in Abelian group of
    points on Elliptic Curve defined by y^2 = x^3 + x over Finite Field in z2 of
    size 23^2
```

1.1.2 Modular curves

A *modular*[24] *curve* is defined as the moduli space of elliptic curves with certain level structure. For example, when we regard $\mathbb{A}^1_{\mathbb{Q}}$ as the moduli space of elliptic curves (isomorphism classes over an algebraically closed field), we obtain the modular curve called *j-line* [KM85, §8.2] [HM98, Exercise 1.6, §2.A] [Wes01, §1] [Hus04, §§4.1, 13.4] [Cla05, Lecture 0, pp. 2–3] [Sai13, §2.1, Example 2.6, Proposition 2.15(1)] [Sai14, Lemma 8.30].

Let $N \geq 1$ be an integer. We define a functor[25] $\mathcal{M}_0(N)_{\mathbb{Z}}$ over $\mathbb{Z}$ by associating to a scheme T the set[26]

$$\mathcal{M}_0(N)_{\mathbb{Z}}(T) = \left\{ \begin{array}{l} \text{isomorphism classes of pairs } (E, C) \text{, such that} \\ E \text{ is an elliptic curve over } T \text{ and} \\ C \text{ is its cyclic subgroup scheme of order } N \end{array} \right\} \tag{11}$$

where two pairs (E, C), (E', C') are isomorphic if there is an isomorphism $\phi : E \to E'$ such that $\phi(C) = C'$ [Sai13, Definition 1.22] [Sai14, Definitions 8.13(2), 8.28(1)]. Then there exists a coarse moduli scheme $Y_0(N)_{\mathbb{Z}}$ of $\mathcal{M}_0(N)_{\mathbb{Z}}$ over $\mathbb{Z}$ such that $Y_0(N)_{\mathbb{Z}}$ is a normal connected affine curve over $\mathbb{Z}$ [Sai13, Definition 2.7] [Sai14, Theorem 8.32(1)]. Then we define the compactification $X_0(N)_{\mathbb{Z}}$ of modular curve $Y_0(N)_{\mathbb{Z}}$ as the integral closure of the j-line [Sai14, Definition 8.62(1)]. $X_0(N)_{\mathbb{Z}}$ is a normal projective curve over $\mathbb{Z}$, and its each geometric fiber is connected [Sai14, Theorem 8.63(1)].

The fiber $Y_0(N) := Y_0(N)_{\mathbb{Q}} = Y_0(N)_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ of $Y_0(N)_{\mathbb{Z}}$ at the generic point is the modular curve $Y_0(N)$ over $\mathbb{Q}$ that is the coarse moduli scheme of the restriction of the functor $\mathcal{M}_0(N)_{\mathbb{Z}}$ to schemes over $\mathbb{Q}$ [Sai13, Definition 2.8(1), Theorem 2.10(2)]. Then $X_0(N)$ is defined as the compactification of $Y_0(N)$ that is a proper smooth curve over $\mathbb{Q}$ [Sai13, Theorem 2.10(2)]. In this report, the algebraic curve $X_0(N)$ will be called the *modular curve of level*[27] N [Sai13, Definition 2.12(1)]. Moreover, using the Riemann-Hurwitz formula we get the genus formula for $X_0(N)$

$$g_0(N) = 1 + \frac{1}{12}\psi(N) - \frac{1}{2}\varphi_\infty(N) - \frac{1}{3}\varphi_6(N) - \frac{1}{4}\varphi_4(N) \tag{12}$$

[24] For a discussion about history of this term see [EvdGM08].

[25] By a "functor over a scheme S" we mean that there is a contravariant functor from the category of schemes over S to the category of sets. Moreover, if $S = \operatorname{Spec} R$ is an affine scheme, a functor over S is called a functor over R [Sai13, Definition 2.3].

[26] As is to be expected, the points of finite order on an elliptic curve, and particularly those of order N, play a decisive role in the study of the modular curves $X_0(N)$, like Mazur's proof of (5) [Ogg75b] [Mor91, §5.6.4] [BM23].

[27] Usually, $X_0(N)$ is called the modular curve of level $\Gamma_0(N)$ over $\mathbb{Q}$, because of the intuitive analytic theory of modular curves we will study next.

where $\psi(N) \coloneqq \#\{\text{cyclic subgroups of order } N \text{ of } \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}\}$, $\varphi_\infty(N) \coloneqq \sum_{d|N} \# \left(\mathbb{Z}/\gcd(d, N/d)\mathbb{Z}\right)^\times$, $\varphi_6(N) \coloneqq \#\{a \in \mathbb{Z}/N\mathbb{Z} \mid a^2 + a + 1 = 0\}$, and $\varphi_4(N) \coloneqq \#\{a \in \mathbb{Z}/N\mathbb{Z} \mid a^2 + 1 = 0\}$ [Sai13, Proposition 2.15(2)] [Col22, §2.1.3] [Inc23, A001617]. In particular, for a prime p we get

$$g_0(p) = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} -1 & \text{if } p \equiv 1 \pmod{12} \\ 0 & \text{if } p = 2, 3;\ p \equiv \pm 5 \pmod{12} \\ 1 & \text{if } p \equiv -1 \pmod{12} \end{cases} \tag{13}$$

which is almost same as (9), hinting towards a relationship between supersingular elliptic curves and modular curves [Sai14, Corollary 8.64].

Furthermore, consider the complex upper half-plane $\mathcal{H} \coloneqq \{\tau \in \mathbb{C} \mid \mathrm{Im}\tau > 0\}$. Let the set of $\mathbb{C}$-valued points on $Y_0(N)$, $Y_0(N)(\mathbb{C})$, consist of the isomorphism classes of the pair $(E_\tau, C_{N,\tau})$, where $\tau \in H$, E_τ is the elliptic curve over $\mathbb{C}$ corresponding to the lattice[28] $\mathbb{Z} + \mathbb{Z}\tau$ in $\mathbb{C}$ and $C_{N,\tau}$ is a cyclic subgroup of order N of E_τ. We can then regard $Y_0(N)(\mathbb{C})$ as the Riemann surface $\Gamma_0(N)\backslash\mathcal{H}$ defined as the left action of

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$$

on $\mathcal{H}$, with the action given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \dfrac{a\tau + b}{c\tau + d}$ [Sai13, Corollary 2.66]. That is, the Riemann surface $Y_0(N)(\mathbb{C})$ is connected and the modular curve $Y_0(N)_\mathbb{C} = Y_0(N) \otimes_\mathbb{Q} \mathbb{C}$ is a connected[29] algebraic curve over $\mathbb{C}$. Then the compactification $X_0(N)_\mathbb{C}$ of modular curve $Y_0(N)_\mathbb{C}$ requires that the cusps be associated with generalized elliptic curves, i.e. curves which are no longer of genus 1 and where a group law can be defined and a distinguished cyclic group of order N can be isolated [Mor91, §5.6.2] [Sai13, §1.5]. In particular, we get

$$X_0(N)(\mathbb{C}) \coloneqq \Gamma_0(N)\backslash\mathcal{H}^*$$

where $\mathcal{H}^* \coloneqq \mathcal{H} \cup \mathbb{P}^1_\mathbb{Q} = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ [DDT95, §1.2] [FM99, §2.1] [Wes01, §2] [Hus04, §11.3] [Loz11, Chapter 3] [Sil09, §C.13] [Loe14, §1.1] [DS16, §2.4] [RS17, Chapter 5] [TVN19, §5.1.1] [Mil21, §V.1] [Col22, §1.3] [Sut22, §18.4, Problem 10.1]. Moreover, every compact Riemann surface has a model as a projective algebraic curve over $\mathbb{C}$, given by polynomial equations [NN01, §I.9.6] [Loe14, Theorem 2.1.1] [Sut22, Remark 19.3]. Such a defining equation[30] of $X_0(N)(\mathbb{C})$ is called *modular polynomial* $\Phi_N(X, Y) \in \mathbb{C}[X, Y]$ defined by

$$\Phi_N(X, j(\tau)) = \prod_{i=1}^{m} (X - j(N\gamma_i\tau))$$

where $\tau \in \mathcal{H}$, $m = [SL_2(\mathbb{Z}) : \Gamma_0(N)]$ and $\Gamma_0(N)\gamma_i$ with $\gamma_i \in SL_2(\mathbb{Z})$ and $i = 1, 2, \ldots, m$, are the right cosets of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$ [DS16, §7.5] [Sut22, §19.2.1] [Cox22, §11.B]. Finally, interpreting $X_0(N)(\mathbb{C})$ as the moduli space of cyclic N-isogenies of elliptic curves over $\mathbb{C}$, for all $j_1, j_2 \in \mathbb{C}$ we have $\Phi_N(j_1, j_2) = 0$ if and only if j_1 and j_2 are the j-invariants of elliptic curves over $\mathbb{C}$ that are related by a cyclic isogeny of degree N [Was08, Theorem 12.5] [Sut22, Theorem 20.3, §20.2] [Cox22, Proposition 14.11].

$X_0(N)(\mathbb{C})$ has the remarkable[31] property that the modular polynomial $\Phi_N \in \mathbb{Z}[X, Y]$ gives a canonical model defined over $\mathbb{Q}$ [Was08, Theorem 10.15] [DS16, §7.6] [TVN19, Theorem 5.1.28] [Mil21, §V.2] [Sut22, Theorem 19.17]. Furthermore, $\Phi_N(X, Y)$ has arithmetic properties like (1) $\Phi_N(X, Y)$ is irreducible when regarded as a polynomial in X; (2) $\Phi_N(X, Y) = \Phi_N(Y, X)$ if $N > 1$; (3) if N is not a perfect square, then $\Phi_N(X, X)$ is a polynomial of degree > 1 with leading coefficient ± 1; and (4) (Kronecker's congruence) if N is a prime[32] p, then $\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \mod p$ [DR73, Théorème VI.6.6] [Loe14, Theorem

[28] A lattice in $\mathbb{C}$ a set $a\mathbb{Z} \oplus b\mathbb{Z}$ [DS16, p. 25]. We will give a general definition in §1.2.2.

[29] Moreover, since $Y_0(N)$ is a dense affine open subscheme of $X_0(N)$, we get that $X_0(N)$ is connected and its field of constants is $\mathbb{Q}$ [Sai13, Theorem 2.10(3)].

[30] This does not mean that $X_0(N)(\mathbb{C})$ is the projective curve given by $\Phi_N(X, Y) = 0$. This curve $\Phi_N(X, Y) = 0$ is highly singular in general, as we will see soon for $\Phi_2(X, Y)$. What we mean is that that the smooth curve $X_0(N)(\mathbb{C})$ is birational to the curve given by $\Phi_N(X, Y) = 0$ [Loe14, §2.2].

[31] There are two reasons. First, in general, a projective algebraic curve over $\mathbb{C}$ can't be defined over $\mathbb{Q}$ (or even $\overline{\mathbb{Q}} = \mathbb{A}$). Second, even if a projective algebraic curve over $\mathbb{C}$ can be defined over $\mathbb{Q}$, in general it can't be defined in any canonical way.

[32] Also note that Φ_p has degree $p + 1$ in each variable because $[SL_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1$ [BSS00, §III.8] [Inc23, A118778].

2.2.1] [Sut22, Theorem 20.7] [Cox22, Theorem 11.18]. These properties of the modular polynomial are straightforward consequences of the properties of the j-function, which makes the modular polynomial seem like a reasonable object to deal with. However, this point of view only holds at the abstract level, but as soon as one asks for concrete examples, the situation gets surprisingly complicated. For example, when $N = 2$ we get

$$\begin{aligned}\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488(X^2Y + XY^2) - 162000(X^2 + Y^2) + 40773375XY +\\ 8748000000(X + Y) - 157464000000000\end{aligned}$$

As can be seen in this example, the integer coefficients of Φ_N are already large when $N = 2$, and they grow rapidly as N increases [Sut22, Example 20.8] [BSS00, §III.8] [Cox22, §13.B]. Fortunately, we now have practical algorithm[33] for computing $\Phi_N(X,Y)$ even when N is well into the thousands [Mil21, Aside V.2.5] [Sut22, Problem 12.2]. Moreover, the curve $\Phi_N(X,Y) = 0$ is highly singular, because without singularities the arithmetic genus formula would predict much too high a genus [Mil21, Remark V.2.6]. For example, we can use SageMath to verify this for $\Phi_2(X,Y) = 0$

```
sage: P2.<X,Y,Z> = ProjectiveSpace(QQ, 2)
sage: ModPoly = ClassicalModularPolynomialDatabase()
sage: Phi2 = ModPoly[2](X,Y)
sage: Phi2
-X^2*Y^2 + X^3 + 1488*X^2*Y + 1488*X*Y^2 + Y^3 - 162000*X^2 + 40773375*X*Y -
    162000*Y^2 + 8748000000*X + 8748000000*Y - 157464000000000
sage: CC = Curve(Phi2.homogenize('Z'), P2)
sage: CC.arithmetic_genus() #[Liu06, Example 7.3.22]
3
sage: CC.genus() #[Liu06, Remark 7.3.28]
0
sage: CC.is_singular()
True
sage: AA = CC.affine_patch(2) #Z=1
sage: AA.is_singular()
True
sage: plot(AA, (X,-10,20000),(Y,-10,20000), axes = True) #real not rational
Graphics object consisting of 1 graphics primitive
```

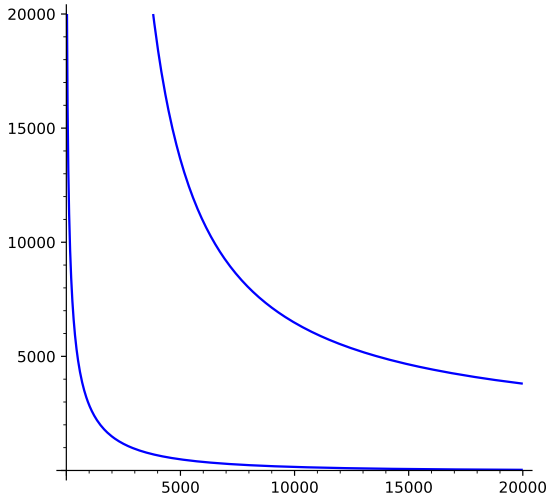


Figure 4: This curve is singular, but appears to be smooth due to the plotting window.

[33] A database of modular polynomials for prime levels computed using [BLS12] and for composite levels N computed using [BOS16, Algorithm 1.1, Corollary 3.4]: `https://math.mit.edu/~drew/ClassicalModPolys.html`

Since $\Phi_2(X,Y) = 0$ is a genus 0 curve, we can use SageMath to find its rational parameterization and visualize the singularity in 3D [Roh97, §1.1] [vHoe97]:

```
sage: #credit:RJ, https://www.math.wustl.edu/~acuna/content/X_0(2).html
sage: #the goal is to visualize the curve in C^2 = R^4
sage: CC.rational_parameterization() #possible because it's genus zero curve
Scheme morphism:
  From: Projective Space of dimension 1 over Rational Field
  To:   Projective Plane Curve over Rational Field defined by -X^2*Y^2 + X^3*Z +
      1488*X^2*Y*Z + 1488*X*Y^2*Z + Y^3*Z - 162000*X^2*Z^2 + 40773375*X*Y*Z^2 -
      162000*Y^2*Z^2 + 8748000000*X*Z^3 + 8748000000*Y*Z^3 - 157464000000000*Z^4
  Defn: Defined on coordinates by sending (s : t) to
        (s^3*t + 768*s^2*t^2 + 196608*s*t^3 + 16777216*t^4 : s^4 + 48*s^3*t +
            768*s^2*t^2 + 4096*s*t^3 : s^2*t^2)
sage: s = var('s')
sage: X = (s^3 + 768*s^2 + 196608*s + 16777216)/(s^2)
sage: Y = (s^4 + 48*s^3 + 768*s^2 + 4096*s)/(s^2)
sage: X = X.numerator().factor()/X.denominator()
sage: Y = Y.numerator().factor()/Y.denominator()
sage: X, Y #beautification
((s + 256)^3/s^2, (s + 16)^3/s)
sage: #checked that we get same 2D curve as above using
sage: #p = parametric_plot((X,Y), (s,-1000,1000))
sage: #show(p, ymin=-10, ymax=20000, xmin=-10, xmax=20000)
sage: s = lambda u,v: (u+i*v)
sage: X = lambda u,v: ((s(u,v) + 256)^3/s(u,v)^2)
sage: Y = lambda u,v: ((s(u,v) + 16)^3/s(u,v))
sage: G0 = (lambda u,v: X(u,v).real(), lambda u,v: X(u,v).imag(), lambda u,v: Y(u
    ,v).real())
sage: cf0 = lambda u,v: Y(u,v).imag() - floor(Y(u,v).imag())
sage: cm0 = colormaps.hsv
sage: pp1 = parametric_plot3d(G0,(-1000,-0.1),(-1000,-0.1),color = (cf0,cm0))
sage: pp1 = pp1.add_condition(lambda X,Y,Z: abs(X)^2+abs(Y)^2+abs(Z)^2 < (20000)
    ^2)
sage: pp2 = parametric_plot3d(G0,(0.1,1000),(0.1,1000),color = (cf0,cm0))
sage: pp2 = pp2.add_condition(lambda X,Y,Z: abs(X)^2+abs(Y)^2+abs(Z)^2< (20000)
    ^2)
sage: show(pp1+pp2, frame=false, viewpoint=[[-0.9521,-0.2128,-0.2196],91.01]) #
    did manual adjustments of viewpoint
None
```

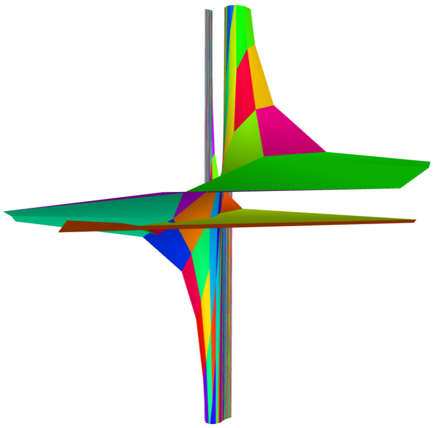


Figure 5: Surface with singularity!

Therefore, the curve $\Phi_N(X,Y)=0$ is a singular affine curve with the same function field as $X_0(N)(\mathbb{C})$ and the desingularization[34] of its projective closure is a smooth projective curve isomorphic to $X_0(N)(\mathbb{C})$ [Ogg80, §2] [Elk98, §3] [Dar09, §3.1] [Loz11, Remark 3.6.4]. For example, SageMath can give a smooth projective model of $X_0(2)(\mathbb{C})$:

```
sage: AA.is_ordinary_singularity([-3375,-3375]) #Phi2(X,Y)=0 by WolframAlpha
True
sage: BB = AA.resolution_of_singularities() #blowing up its singular points
sage: BB[0][0] #1st affine patch of the resolution of singularity
Affine Plane Curve over Rational Field defined by X^2*s1^2 - X*s1^3 - 1488*X*s1^2
    - 3375*s1^3 - 8238*X*s1 + 172125*s1^2 - X - 2926125*s1 + 16581375
sage: ##BB[0][1] #2nd affine patch of the resolution of singularity
sage: ##BB[1][0][0] #transition map from the 1st patch to itself
sage: BB[1][0][1] #transition map from the 1st patch to the 2nd patch
Scheme morphism:
  From: Affine Plane Curve over Rational Field defined by X^2*s1^2 - X*s1^3 -
       1488*X*s1^2 - 3375*s1^3 - 8238*X*s1 + 172125*s1^2 - X - 2926125*s1 +
       16581375
  To:   Affine Plane Curve over Rational Field defined by Y^2*s0^2 - Y*s0^3 -
       1488*Y*s0^2 - 3375*s0^3 - 8238*Y*s0 + 172125*s0^2 - Y - 2926125*s0 +
       16581375
  Defn: Defined on coordinates by sending (X, s1) to
          (X*s1 + 3375*s1 - 3375, 1/s1)
sage: ##BB[1][1][0] #transition map from the 2nd patch to the 1st patch
sage: ##BB[1][1][1] #transition map from the 2nd patch to itself
sage: BB[2][0] #birational map from the 1st patch to the original curve
Scheme morphism:
  From: Affine Plane Curve over Rational Field defined by X^2*s1^2 - X*s1^3 -
       1488*X*s1^2 - 3375*s1^3 - 8238*X*s1 + 172125*s1^2 - X - 2926125*s1 +
       16581375
  To:   Affine Plane Curve over Rational Field defined by -X^2*Y^2 + X^3 + 1488*X
       ^2*Y + 1488*X*Y^2 + Y^3 - 162000*X^2 + 40773375*X*Y - 162000*Y^2 +
       8748000000*X + 8748000000*Y - 157464000000000
  Defn: Defined on coordinates by sending (X, s1) to
          (X, X*s1 + 3375*s1 - 3375)
sage: ##BB[2][1] #birational map from the 2nd patch to the original curve
```

Next, for a prime number p, we denote by $\mathcal{M}_0(N)_{\mathbb{F}_p}$ the restriction of the functor $\mathcal{M}_0(N)_{\mathbb{Z}}$ to schemes over $\mathbb{F}_p$. If $p \nmid N$ then $Y_0(N)_{\mathbb{F}_p} = Y_0(N)_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$ is the coarse moduli scheme of the restriction $\mathcal{M}_0(N)_{\mathbb{F}_p}$ [Sai14, Theorem 8.32(3)]. Moreover, for $p \nmid N$, $X_0(N)_{\mathbb{Z}}$ is smooth at p and the fiber $X_0(N)_{\mathbb{F}_p} = X_0(N)_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$ is a smooth compactification of $Y_0(N)_{\mathbb{F}_p}$ [Sai14, Theorem 8.63(2)]. Furthermore, Igusa [Igu59] proved that $X_0(N)(\mathbb{C})$ has a non-singular projective model over $\mathbb{Q}$ whose reduction modulo primes p, $p \nmid N$, are also non-singular [Mor91, Theorem 5.9] [Ogg80, §4] [Hus04, Remark 16.7.1] [RS17, §12.6] [TVN19, Theorem 5.1.30]. Therefore, if K is a field of characteristic not dividing N, then for all $j_1, j_2 \in K$ we have $\Phi_N(j_1,j_2)=0$ if and only if j_1 and j_2 are the j-invariants of elliptic curves over K that are related by a cyclic isogeny of degree N defined[35] over K [Sut22, Theorem 20.4]. In particular, for a prime $\ell \neq p$, if E_1, E_2 are elliptic curves with j-invariants $j_1, j_2 \in \overline{\mathbb{F}}_p$ then $\Phi_\ell(j_1,j_2)=0$ if and only if there is an ℓ-isogeny $E_1 \to E_2$ [Was08, Theorem 12.19]. That is, if K is a field of characteristic p and ℓ is a prime different from p, then for any fixed j-invariant $j_1 := j(E_1)$, the K-rational roots of the $(\ell+1)$-degree[36] polynomial $\Phi_\ell(j_1,Y)$ are the j-invariants

[34] However, such models are not useful for finding isogenous elliptic curves because there is no obvious way to use these models to find a polynomial analogous to the $\Phi_N(j(E),Y)$ mentioned above [Gal96, Chapter 1]. Moreover, since $X_0(N)(\mathbb{C})$ will always have at least one rational point (the cusp at infinity) the curves of genus 1 will always be elliptic curves. In fact, the modularity theorem states that every elliptic curve defined over $\mathbb{Q}$ is parameterized by some modular curve $X_0(N)$ [Gal96, §2.6] [Elk98, §3] [DS16, Theorem 7.7.2].

[35] If K is not algebraically closed then it is not necessarily true that $\Phi_N(j(E_1),j(E_2))=0$ implies the existence of a cyclic N-isogeny $E_1 \to E_2$ over K [Col22, Theorem 2.31] [Sut22, Remark 20.5].

[36] Note that there are $\ell+1$ separable isogenies of degree ℓ (not necessarily defined over K) from E to other curves (some of these isogenies may map to the same image curve), because there are $\ell+1$ different (cyclic) order ℓ subgroups of $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$:

of the elliptic curves E_2 over K that are ℓ-isogenous to E_1 [BSS00, §III.8] [Hus04, Assertion 11.9.5] [Gal12, §25.1]. For example, SageMath uses this to list all (separable) 2-isogenies from $E : y^2 = x^3 + x$ over $\mathbb{F}_{23}$ and $\mathbb{F}_{23^2}$ [Ban+19, Corollary 2.5]:

```
sage: E0.isogenies_prime_degree(2) #we don't get all three
[Isogeny of degree 2 from Elliptic Curve defined by y^2 = x^3 + x over Finite
   Field of size 23 to Elliptic Curve defined by y^2 = x^3 + 19*x over Finite
   Field of size 23]
sage: E0.change_ring(GF(23^2)).isogenies_prime_degree(2) #we get all three
[Isogeny of degree 2 from Elliptic Curve defined by y^2 = x^3 + x over Finite
   Field in z2 of size 23^2 to Elliptic Curve defined by y^2 = x^3 + 19*x over
   Finite Field in z2 of size 23^2, Isogeny of degree 2 from Elliptic Curve
   defined by y^2 = x^3 + x over Finite Field in z2 of size 23^2 to Elliptic
   Curve defined by y^2 = x^3 + 11*x + (16*z2+7) over Finite Field in z2 of size
   23^2, Isogeny of degree 2 from Elliptic Curve defined by y^2 = x^3 + x over
   Finite Field in z2 of size 23^2 to Elliptic Curve defined by y^2 = x^3 + 11*x
   + (7*z2+16) over Finite Field in z2 of size 23^2]
```

Next, if $N = N'N''$ with $\gcd(N', N'') = 1$, we have an identification [Sai14, p. 22]

$$\mathcal{M}_0(N'N'')(T) = \left\{ \begin{array}{l} \text{isomorphism classes of triples } (E, C', C''), \text{ such that} \\ E \text{ is an elliptic curve over } T, \\ C' \text{ is its cyclic subgroup scheme of order } N', \text{ and} \\ C'' \text{ is its cyclic subgroup scheme of order } N'' \end{array} \right\} \tag{14}$$

In particular, for $N = Mp$ such that $M \geq 1$ is an integer relatively prime to p, we get the following identification for a scheme T over $\mathbb{F}_p$

$$\mathcal{M}_0(Mp)_{\mathbb{F}_p}(T) = \left\{ \begin{array}{l} \text{isomorphism classes of triples } (E, C', C''), \text{ such that} \\ E \text{ is an elliptic curve over } T, \\ C' \text{ is its cyclic subgroup scheme of order } M, \text{ and} \\ C'' \text{ is its cyclic subgroup scheme of order } p \end{array} \right\} \tag{15}$$

Then define a *Frobenius morphism* of functors $F : \mathcal{M}_0(Mp)_{\mathbb{F}_p} \to \mathcal{M}_0(Mp)_{\mathbb{F}_p}$ by associating the isomorphism class of a pair (E, C) with the isomorphism class of $(E^{(p)}, C^{(p)})$, where $E^{(p)}$ and $C^{(p)}$ are defined as the fiber products $E \times_T T$ and $C \times_T T$ by the absolute frobenius morphism $\pi : T \to T$ [Sai14, p. 23]. Also, let $V : \mathcal{M}_0(Mp)_{\mathbb{F}_p} \to \mathcal{M}_0(Mp)_{\mathbb{F}_p}$ be the dual *Verschiebung morphism* defined by associating the isomorphism class of a pair $(E^{(p)}, C^{(p)})$ with the isomorphism class of (E, C). We can then define a morphism of functors over $\mathbb{F}_p$, $j_F : \mathcal{M}_0(M)_{\mathbb{F}_p} \to \mathcal{M}_0(Mp)_{\mathbb{F}_p}$ by associating to the isomorphism class of a pair (E, C) the isomorphism class of $(E, C, \ker F)$. We can also define $j_V : \mathcal{M}_0(M)_{\mathbb{F}_p} \to \mathcal{M}_0(Mp)_{\mathbb{F}_p}$ by associating to the isomorphism class of a pair (E, C) the isomorphism class of $(E^{(p)}, C^{(p)}, \ker V)$ [DR73, p. V.1.15] [Sai14, p. 23]. Then the morphisms $j_F, j_V : \mathcal{M}_0(M)_{\mathbb{F}_p} \to \mathcal{M}_0(Mp)_{\mathbb{F}_p}$ over $\mathbb{F}_p$ induce closed immersions $j_F, j_V : Y_0(M)_{\mathbb{F}_p} \to Y_0(Mp)_{\mathbb{Z}}$, such that the fiber $Y_0(Mp)_{\mathbb{F}_p} = Y_F \cup Y_V$ and $Y_F = Y_0(M)_{\mathbb{F}_p}$ for $Y_F = j_F(Y_0(M)_{\mathbb{F}_p})$ and $Y_V = j_V(Y_0(M)_{\mathbb{F}_p})$ [DR73, Théorème V.1.16] [Sai14, Theorem 8.32(4)]. Furthermore, since the closures $\overline{Y_F}, \overline{Y_V}$ of the images of the closed immersions $j_F, j_V : Y_0(M)_{\mathbb{F}_p} \to Y_0(Mp)_{\mathbb{Z}}$ are regular at the cusps, both are isomorphic to $X_0(M)_{\mathbb{F}_p}$. Thus the closed immersions j_F and j_V extend to closed immersions $j_F, j_V : X_0(M)_{\mathbb{F}_p} \to X_0(Mp)_{\mathbb{F}_p}$ such that $X_0(Mp)_{\mathbb{F}_p} = \overline{Y_F} \cup \overline{Y_V} \cong X_0(M)_{\mathbb{F}_p} \cup X_0(M)_{\mathbb{F}_p}$ [Sai14, Theorem 8.63(3)]. In particular, for $M = 1$, $X_0(p)_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ is the union of two copies of $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$, as predicted by the Kronecker's congruence relation for modular polynomial Φ_p [DR73, Théorème VI.6.9(ii), Example VI.6.16] [KM85, Introduction] [Mor91, Figure 5.10] [DDT95, §1.5] [Elk98, §4] [Loe14, §2.2].

We define a subfunctor $\mathcal{M}_0(M)^{ss}_{\mathbb{F}_p}$ of $\mathcal{M}_0(M)_{\mathbb{F}_p}$ $(p \nmid M)$ by associating to a scheme T over $\mathbb{F}_p$ the set

$$\mathcal{M}_0(M)^{ss}_{\mathbb{F}_p}(T) = \left\{ \begin{array}{l} \text{isomorphism classes of pairs } (E, C), \text{ such that} \\ E \text{ is a supersingular elliptic curve over } T \text{ and} \\ C \text{ is its cyclic subgroup scheme of order } M \end{array} \right\} \tag{16}$$

https://proofwiki.org/wiki/Non-Cyclic_Group_of_Order_p%5E2_has_p%2B3_Subgroups where for a field K of characteristic p and $T = \operatorname{Spec} K$ we recover the definition of supersingular elliptic curves over K from §1.1.1 [Sai14, §8.1, eq. 8.29]. Then $Y_F \cap Y_V = \overline{Y_F} \cap \overline{Y_V}$ is the coarse moduli $Y_0(M)^{ss}_{\mathbb{F}_p}$ of $\mathcal{M}_0(M)^{ss}_{\mathbb{F}_p}$ [Sai14, Theorems 8.32(4) and 8.63(3)]. That is, coincidentally[37], the points on the modular curve $Y_0(Mp)_{\mathbb{F}_p}$ ($p \nmid M$) corresponding to supersingular elliptic curves coincide with the singular points of this modular curve. Therefore, $X_0(Mp)_{\mathbb{F}_p}$ can be viewed as two copies of $X_0(M)_{\mathbb{F}_p}$ glued at the "supersingular points" [DR73, Variante V.1.18] [KM85, Theorem 12.4.5, §13.1.6] [Wei13] [Has97, Fig. 1] [RS17, Figure 12.6.1] [Ari19, §2.1]. We can then define the module of divisors on the modular curve $X_0(Mp)_{\mathbb{F}_p}$ over $\mathbb{F}_p$ supported at supersingular points[38]. That is, for $N = Mp$, we define *supersingular module* $\mathbf{M}_N = \oplus_S \mathbb{Z}[S]$ where S is taken over all supersingular points of $X_0(M)_{\mathbb{F}_p}$ in characteristic p [Mes86, §2.1] [Rib90, Proposition 3.1] [Déc98, §2.3] [Koh01, §3.1] [Eme02, §3].

In particular, for $M = 1$, since $X_0(p)_{\mathbb{F}_p} = \overline{Y_F} \cup \overline{Y_V}$ is connected[39], we have $\overline{Y_F} \cap \overline{Y_V} = Y_0(1)^{ss}_{\mathbb{F}_p} \neq \emptyset$. Moreover, we have

$$\left\{\begin{matrix}\text{isomorphism classes} \\ \text{of supersingular} \\ \text{elliptic curves over } \overline{\mathbb{F}}_p\end{matrix}\right\} = \mathcal{M}_0(1)^{ss}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p) = Y_0(1)^{ss}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$$

with $\#Y_0(1)^{ss}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p) = g_0(p) + 1$ [Ogg75a, eq. 14] [Sai14, Corollary 8.64]. Therefore, the number isomorphism classes of supersingular elliptic curves in characteristic p is precisely one more than the genus of the modular curve $X_0(p)$ [DR73, Corollaire VI.6.11] [Ogg80, eq. 18] [DI95, §9.3] [Elk98, §4] [Voi05, Proposition 3.1] [Cla05, Lecture 1, p. 9] [DJP14, §2.2] [Sou16, §4.1.2]. Finally, combining this with (13) we obtain (9). For example, $S_{23} = 1 + g_0(23) = 1 + 2 = 3$ [RS17, Example 13.5.3], and we can use SageMath to verify this:

```
sage: SM = SupersingularModule(23)
sage: SM
Module of supersingular points on X_0(1)/F_23 over Integer Ring
sage: SM.dimension() #the number of supersingular points
3
```

Using (14), for $N = N'N''$ with $\gcd(N', N'') = 1$, we can associate to the isomorphism class of triples (E, C', C'') the isomorphism class of triples[40] $(E/C', E[N']/C', (C'' + C')/C')$, to obtain a morphism of functors $w_{N'} : \mathcal{M}_0(N'N'') \to \mathcal{M}_0(N'N'')$ called *Atkin-Lehner involution*, where $w_{N'}^2$ is the identity [Sai14, pp. 22-23] [DR73, §IV.4.4]. We can similarly define $w_{N''}$. In particular, for $N = Mp$ as in (15), we have the Atkin–Lehner involution $w_p : X_0(Mp)_{\mathbb{F}_p} \to X_0(Mp)_{\mathbb{F}_p}$. Note that $w_p(E, C, \ker F) = (E/\ker F, E[p]/\ker F, (C + \ker F)/\ker F) = (E^{(p)}, C^{(p)}, \ker F)$. In particular, the action of w_p on supersingular points $X_0(M)^{ss}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ equals the action of F. Moreover, w_p permutes irreducible components[41] of $X_0(Mp)_{\mathbb{F}_p}$ and F preserves irreducible components [DR73, §VI.6.1] [Ogg75a, §3] [Sai14, p. 100]. Therefore, we recover the familiar fact that all supersingular points of $X_0(M)^{ss}_{\mathbb{F}_p}$ are defined over $\mathbb{F}_{p^2}$ [Ogg80, §4] [Mes86, §2.1]. Furthermore, w_p exchanges each supersingular point which is properly $\mathbb{F}_{p^2}$-rational with its conjugate, while it fixes each $\mathbb{F}_p$-rational supersingular point [HH96, Appendix C]. We then write $\#X_0(M)^{ss}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p) = r_p(M) + 2s_p(M)$, where r_p is the number of points rational over $\mathbb{F}_p$, and s_p is the number of conjugate pairs in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ [Ogg80, eq. 20]. In particular, for $M = 1$, we get that $1 + g_0(p) = r_p + 2s_p$ [Ogg75a, §3]. Therefore, the quotient[42] $X_0^+(p) := X_0(p)/w_p$ is a line with s_p ordinary double points [HH96, Fig. 1]. That is, the genus $g_0^+(p)$ of $X_0^+(p)$ is s_p, and $2g^+(p)$ is the number of supersingular j-invariants in

[37] The term "supersingular" was not defined defined to justify this relation with "singular" points. We will discuss the origin of this term in §1.3.

[38] We will learn to find these supersingular points in §1.3.

[39] Note that by [Sai14, Theorem 8.63(1)] each fiber of $X_0(N)_{\mathbb{Z}}$ is connected.

[40] Since E is an elliptic curve over T and N is a positive integer, the multiplication-by-N morphism $[N] : E \to E$ is characterized by the condition that for any scheme S over T, the induced mapping $[N] : E(S) \to E(S)$ is the multiplication-by-N mapping of the commutative group $E(S)$ [Sai13, Proposition 1.26]. Moreover, the kernel $E[N] = [N]^{-1}0$ of the multiplication-by-N morphism $[N] : E \to E$ is the fibered product over E of $[N] : E \to E$ and the 0-section: $T \to E$ [Sai13, Corollary 1.27].

[41] In other words, w_p maps a cyclic p-isogeny $E \to E'$ to the dual isogeny $E' \to E$ [Jao03, p. 2] [DR73, §IV.4.5].

[42] In other words, the quotient space $X_0^+(p)$ parametrizes cyclic p-isogenous curves $\{E, E'\}$ instead of p-isogenies $E \to E'$ [Jao03, p. 2].

$\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ [Ogg75a, eq. 15]. On the other hand, using the Riemann-Hurwitz formula we get

$$g_0^+(p) = \frac{g_0(p)+1}{2} - \frac{\nu(w_p)}{4}$$

where $\nu(w_p)$ is the number of fixed points of w_p [Ogg74, §§1, 2] [Ogg75a, eq. 2, 3] [Ogg75b, eq. 8, 9] [Ken77] [Ogg80, eq 15] [FH99, §1] [Col22, pp. 59–60]. Therefore, $g_0^+(p) = 0$ iff $g_0(p) = 0$, i.e. $p \in \{2, 3, 5, 7, 13\}$ [Inc23, A091401]; or $g_0(p) = 1$, i.e. $p \in \{11, 17, 19\}$ [Inc23, A091403]; or $g_0(p) \geq 2$ such that w_p is equal to hyperelliptic involution[43], i.e. $p \in \{23, 29, 31, 41, 47, 59, 71\}$ [Inc23, A276182]; [Ogg75a, Corollaire] [Ogg80, eq. 24] [Jao03, §2.2] [Col22, Corollary 2.50]. Moreover, these fifteen primes

$$\mathbb{S} := \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$$

form the set of *supersingular primes*[44] because all the supersingular j-invariants in characteristic $p \in \mathbb{S}$ are in the prime field $\mathbb{F}_p$ [Ogg75a, eq. 16] [Ari19] [Haj23, Remark 3.0.1] [Inc23, A002267]. For example, since $23 \in \mathbb{S}$, we expect all the j-invaraints to lie in $\mathbb{F}_{23}$, as verified using SageMath:

```
sage: SM.supersingular_points()[0] #the list of supersingular j-invariants
[3, 19, 0]
```

Furthermore, from the example following (9), we know that the isomorphism classes of supersingular elliptic curves are represented by $E_1 : y^2 = x^3 + x$, $E_2 : y^2 = x^3 + 1$ and $E_3 : y^2 = x^3 - 4x^2 + 3x$. We can use SageMath to match them with the j-invariant labels listed above:

```
sage: E0.j_invariant()
3
sage: EllipticCurve(GF(23), [0,-4,0,3,0]).j_invariant()
19
sage: EllipticCurve(GF(23), [0,0,0,0,1]).j_invariant()
0
```

Moreover, since $g_0(23) = 2$, $X_0(23)(\mathbb{C})$ has a hyperelliptic equation[45] over $\mathbb{Q}$ given by $y^2 = f(x)$ where

$$f(x) = x^6 - 8x^5 + 2x^4 + 2x^3 - 11x^2 + 10x - 7 = (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$$

This equation can be computed by various methods[46] [Mur92, Table 1] [Shi95, §4] [Gal96, Table 3] [Sch12, §1]. However, for genus 2 curves we can't have a non-singular[47] model in $\mathbb{P}^2_{\mathbb{C}}$. Therefore, we generally use a plane hyperelliptic equation which represents the image of a projection $X_0(23)(\mathbb{C}) \to \mathbb{P}^2_{\mathbb{C}}$ such that the image curve in $\mathbb{P}^2_{\mathbb{C}}$ has a single singularity at infinity [Gal96, p. 5 and 10] [Gal12, §10.1]. We can verify this using SageMath:

```
sage: R.<x> = QQ[] #polynomial ring
sage: H = HyperellipticCurve(x^6 - 8*x^5 + 2*x^4 + 2*x^3 - 11*x^2 + 10*x - 7)
sage: H
```

[43] A curve C over K, of genus $g \geq 2$, is *hyperelliptic* if it has a function $F : X \to \mathbb{P}^1_K$ of degree 2, i.e. it has a hyperelliptic involution v such that C/v is of genus 0 [Ogg75a, p. 7-02] [Mir95, Prop III.4.11] [Gal96, §2.6] [Liu06, Definition 7.4.27, Prop 7.4.29] [Gal12, Definition 10.0.1]. There are only eight primes for which the modular curve $X_0(p)$ is hyperelliptic, and among these only $p = 37$ has exceptional hyperelliptic involution [Ogg74, Theorem 2] [Ogg80, §5] [Col22, Prop 2.51] [BM23, §10].

[44] There are two notions of "supersingular prime": one is absolute, and one is relative to a fixed elliptic curve. What we defined here is an absolute notion, a list of fifteen primes. Later, in §1.3, we will define the relative notion. In fact, the supersingular primes for elliptic curves over $\mathbb{Q}$ is not finite. Also see this discussion on MathOverflow: `https://mathoverflow.net/a/1339`.

[45] Let C be a hyperelliptic curve of genus g over a field K. Then $y^2 + h(x)y = f(x)$, $f(x), h(x) \in k[x]$ with $2g + 1 \leq \max\{2\deg(h), \deg(f)\} \leq 2g + 2$ is called a *hyperelliptic equation* of C [Mir95, Def III.1.8] [Gal96, §2.6] [Liu06, Def 7.4.32].

[46] We can also get the hyperelliptic model $y^2 = g(x)$ where $g(x) = f(x+2) = x^6 + 4x^5 - 18x^4 - 142x^3 - 351x^2 - 394x - 175 = (x^3 - 2x^2 - 17x - 25)(x^3 + 6x^2 + 11x + 7)$ [Rov91, §4.3, p. 794] [FM99, Table 5.4, p. 44]. For a general discussion on finding equations for modular curves, see [Mes86, Appendice] [Elk98, §4], [Col22, §2.2.7, Appendix A] and [Roe23].

[47] A plane curve has a degree d and if it is smooth its genus is then $g = \frac{1}{2}(d-1)(d-2)$ [Liu06, Example 7.3.22]. However, since most integers are not of the form $\frac{1}{2}(d-1)(d-2)$, most smooth curves are non-planar. That is, no smooth curve of genus 2 is planar [Mir95, Proposition VII.1.10] [Liu06, Proposition 7.4.9]. Moreover, genus 3 hyperelliptic curves are non-planar because they have degree either 7 or 8 [Mir95, Proposition VII.2.5].

```
Hyperelliptic Curve over Rational Field defined by y^2 = x^6 - 8*x^5 + 2*x^4 + 2*
    x^3 - 11*x^2 + 10*x - 7
sage: #H.is_singular() will always return False because HyperellipticCurve
    constructor ensures that there are no unwanted singularities
sage: from sage.schemes.curves.projective_curve import ProjectivePlaneCurve
sage: ProjectivePlaneCurve.is_singular(H)
True
sage: from sage.schemes.curves.affine_curve import AffineCurve
sage: AffineCurve.is_singular(H.affine_patch(2))
False
sage: plot(H) #affine plot over real numbers instead of rationals
Graphics object consisting of 1 graphics primitive
```

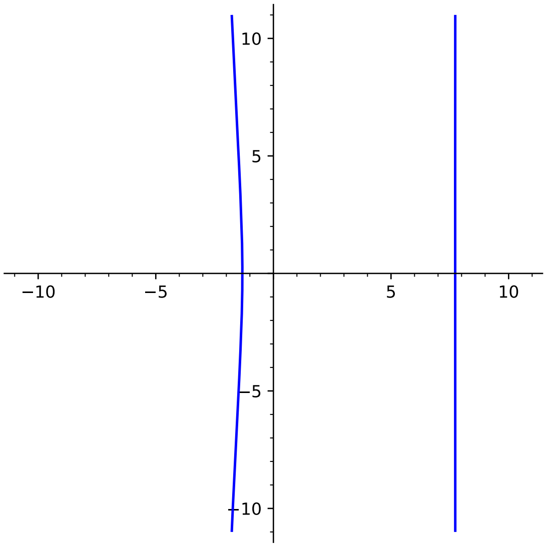


Figure 6: Note that $f(x) = 0$ has two real roots and the curve does not exist between them.

1.1.3 Drawing graphs

Let ℓ be a prime different from p. The *supersingular ℓ-isogeny graph*[48] in characteristic p is the directed multigraph $G_\ell(p)$ whose vertices belong to the set of supersingular points $\{j \in \mathbb{F}_{p^2} \mid \ E(j) \text{ is supersingular}\}$ where $E(j)$ is the curve defined by the equation[49]

$$\begin{aligned}
y^2 + xy &= x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728} && \text{if } j \neq 0, 1728,\\
y^2 + y &= x^3 && \text{if } j = 0,\\
y^2 &= x^3 + x && \text{if } j = 1728,
\end{aligned}$$

and the number of directed edges from j to j' is equal to the multiplicity of j' as a root of $\Phi_\ell(j, Y)$ in $\mathbb{F}_{p^2}$ [GV18, §6] [Ban+19, Definition 2.1]. That is, the vertex set of $G_\ell(p)$ corresponds to the $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and every edge $[j, j']$ corresponds to a cyclic ℓ-isogeny $E(j) \to E(j')$ over $\overline{\mathbb{F}}_p$ [Arp+21, Definition 2.2].

Note that, from (9) we get that $G_\ell(p)$ has approximately $p/12$ vertices. Moreover, since $\Phi_\ell(j, Y)$ is a $(\ell + 1)$-degree polynomial in Y, every vertex of $G_\ell(p)$ has outgoing degree $\ell + 1$. Furthermore, $G_\ell(p)$ is

[48] This is a special case of the more general definition given in [Sut13] [Sut22, Lecture 22, Problem 12.3].

[49] Note that in characteristic 2 or 3 we have $1728 = 0$, so even in these cases one of the two curves will be nonsingular and fill in the missing value of j [Sil09, Proposition III.1.4(c)] Furthermore, for $p \geq 5$, $j = 0$ is supersingular iff $p \equiv 2 \pmod 3$ and $j = 1738$ is supersingular iff $p \equiv 3 \pmod 4$ [Sil09, Examples V.4.4, V.4.5].

connected[50] because $\ell+1$ has multiplicity 1 as an eigenvalue of the adjacency matrix of $G_\ell(p)$ [Mes86, §2.4]. Therefore, for all primes ℓ, the diameter of $G_\ell(p)$ is $O(\log p)$, where the constant in the bound is independent of ℓ, i.e. the shortest path between any two vertices has length $O(\log p)$ [Koh96, Theorem 79]. For example, we can use SageMath to draw $G_2(23)$ [vdLaa18, §7.1] [GV18, Figure 1 and 2] [Ban+19, §6]:

```
sage: M = SM.hecke_matrix(2) #the action of the Hecke operator T_2 on S
sage: M
[1 2 0]
[1 1 1]
[0 3 0]
sage: SM.supersingular_points()[1] #rows and column indexes of M follow this
    ordering
{3: 0, 19: 1, 0: 2}
sage: G = DiGraph(M, format=’adjacency_matrix’)
sage: GG = G.graphplot(pos=dict(zip(G, [[-1,0], [1,0], [0,-2]])), vertex_labels=
    dict(zip(G, [’3’, ’19’, ’0’])), vertex_size=4000, dist=2, loop_size=0.2,
    edge_thickness=2)
sage: GG.plot()
Graphics object consisting of 15 graphics primitives
```

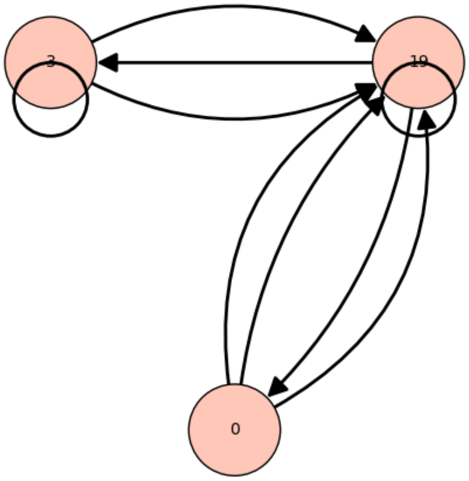


Figure 7: Supersingular 2-isogeny graph in charateristic 23

1.2 ℓ-Brandt graphs

1.2.1 Quaternion algebras

A *quaternion algebra* B over K is a central simple K-algebra[51] with $\dim_F B = 4$ (as a K-vector space) [Déc98, Definition 1.3] [Voi13, Definition 1.9] [Mar17, Definition 3.1.1] [Ver23, §2.3.3]. Then, either $B \cong M_2(K)$ (matrix K-algebra), called *split*, or B is a skew field (division K-algebra) [Déc98, Lemma 1.30] [Voi21,

[50] The number of connected components of a m-regular graph G is the dimension of the eigenspace for m in the adjacency matrix for G [DSV03, Proposition 1.1.2] [BH12, Proposition 1.3.8] [Mar14, Proposition 3.2.12]. The adjacency matrix of $G_\ell(p)$ defines the action of the Hecke operator T_ℓ, and the 1-dimensional space of Eisenstein series is the eigenspace for $\ell+1$ (regular out-degree) [Koh96, Note on p. 89].

[51] That is, B is an associative ring with 1 equipped with an embedding $K \hookrightarrow B$ of rings (taking $1 \in K$ to $1 \in B$) whose image lies in the center of B, i.e. $K \subseteq Z(B) \coloneqq \{\alpha \in B \mid \alpha\beta = \beta\alpha \ \forall\, \beta \in B\}$; we identify K with its image under this embedding. Here B is central, i.e. $Z(B) = K$; and simple, i.e. the only two-sided ideals of B are $\langle 0 \rangle$ and B (or equivalently that any K-algebra homomorphism with domain B is either the zero map or injective). Moreover, a 4-dimensional central division K-algebra is isomorphic to a quaternion algebra [GS17, Proposition 1.2.1] [Voi21, Cor 7.1.2, Prop 7.6.1.].

Proposition 7.6.2]. In particular, if K is an algebraically closed field then $B \cong M_2(K)$ [Déc98, Theorem 1.32] [GS17, Corollary 2.1.7].

Moreover, B is a quaternion algebra iff there is a separable quadratic K-algebra[52] A for which there exists $b \in K^\times$ and $j \in B$ such that $B = A \oplus Aj$ as a left K-vector space with basis $\{1, j\}$ with the multiplication rules $j^2 = b$ and $j\alpha = \overline{\alpha}j$ for $\alpha \in A$, where $\overline{}$ is the standard involution[53] on A [Déc98, Remark, pp. 4–5] [AB04, p. 2] [Voi13, Lemma 2.11] [Voi21, Definition 6.1.5]. We use the notation, $B \coloneqq (A, b \mid K)$, such that $(A, b \mid K) \cong (A, b' \mid K)$ iff $b/b' \in \mathrm{Nm}_{A/K}(A^\times)$ [Voi21, Cor 7.6, Def 16.4.1]. Thus, the maximal subfields of a quaternion algebra are quadratic [Mar17, Exercise 3.1.2] [Voi21, Corollary 7.7.11] [Ver23, Figure 2.2].

Let B be a quaternion algebra over a local field[54] K. Then the *classification theorem of quaternion algebras over local fields* states that, up to K-algebra isomorphism, we have

$$\begin{array}{ll} B \cong \mathbb{H} \coloneqq (\mathbb{C}, -1 \mid \mathbb{R}) \text{ or } B \cong M_2(\mathbb{R}) & \text{if } K = \mathbb{R} = \mathbb{Q}_\infty \\ B \cong M_2(\mathbb{C}) & \text{if } K = \mathbb{C} \\ B \cong (K^{un,2}, \varpi \mid K) \text{ or } B \cong M_2(K) & \text{if } K \text{ is nonarchimedean} \end{array}$$

where $K^{un,2}$ is the unique quadratic unramified[55] extension of K and ϖ is the uniformizer of K [Déc98, §1.3] [AB04, p. 2] [Mar17, §5.1] [Voi21, §12.3, 13.3]. For example, the unique division quaternion algebra B over $\mathbb{Q}_p$, up to isomorphism, is given by $B \cong (\mathbb{Q}_{p^2}, p \mid \mathbb{Q}_p)$, where $\mathbb{Q}_{p^2}$ is the unique unramified quadratic extension[56] of $\mathbb{Q}_p$ [Voi21, §13.1].

Let B be a quaternion algebra over a global field[57] K with the set of places $\mathrm{Pl}(K)$. We say that B is *ramified* (unramified/split) at $v \in \mathrm{Pl}(K)$ if $B_v \coloneqq B \otimes_K K_v$ is a division K_v-algebra (matrix K_v-algebra), where K_v is the local field that is completion[58] of K with respect to v [Déc98, Definition 1.48] [AB04, Definition 1.7] [Voi21, Definition 14.5.1, Remark 14.5.2]. Note that, as per the discussion in previous paragraph, B can only ramify at non-complex. Let $\mathrm{Ram}(B)$ denote the set of ramified places of B. Then the *classification theorem of quaternion algebras over global fields* states that $\mathrm{Ram}(B)$ is a finite set of even cardinality that uniquely determines B up to K-isomorphism, and every such set occurs [Déc98, Theorem 1.52] [AB04, Theorem 1.8] [Voi21, Main Theorem 14.6.1]. We define the *discriminant*[59] $\mathrm{disc}(B)$ of B to be the product of prime ideals corresponding to the finite places in $\mathrm{Ram}(B)$ [Déc98, Definition 1.50] [AB04, Definition 1.9] [Voi21, Definition 14.5.4]. That is, two quaternion K-algebras are isomorphic if and only if they have the same discriminant [GV11, Algorithm 4.1] [Voi21, Proposition 14.2.7]. Moreover, if K is a totally real number field then we say that B is *definite* if all real places of K are ramified in B, otherwise, we say B is *indefinite* [AB04, Definition 1.17] [Voi21, Definition 14.5.7]. For example, for $K = \mathbb{Q}$, the definite or indefinite classification of a quaternion $\mathbb{Q}$-algebra B can be read off from the discriminant $\mathrm{disc}(B)$, i.e. an odd number of factors of $\mathrm{disc}(B)$ corresponds to the definite case, and an even number to the indefinite case [AB04, p. 5].

Finally, we give a concrete description of a quaternion K-algebra B [Déc98, Remark, p. 5]. Using this characterization, we can show that any quaternion algebra over a finite field is split [Voi21, Exercises 3.16,

[52] That is, A is an associate K-algebra such that $\dim_K A = 2$ (i.e. commutative [Voi21, Lemma 3.4.2]) and $A \otimes_K \overline{K} \cong \overline{K} \times \overline{K}$ [Voi21, §6.1][Rei03, §7c].

[53] An *involution* $\overline{} : A \to A$ is a K-linear map which satisfies: (1) $\overline{1} = 1$; (2) $\overline{\overline{\alpha}} = \alpha$ for all $\alpha \in A$; and (3) $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ [Voi21, Definition 3.2.1]. An involution is *standard* if $\alpha\overline{\alpha} \in K$ for all $\alpha \in A$ [Voi21, Definition 3.2.4]. Moreover, since A is a quadratic K-algebra, it has a unique standard involution [Voi21, Lemma 3.4.2].

[54] The archimedean local fields are $\mathbb{R}$ and $\mathbb{C}$. The nonarchimedean local fields are the finite extensions of the $\mathbb{Q}_p$ (characteristic 0) and $\mathbb{F}_p((t))$ (characteristic p). Note that $\overline{\mathbb{Q}}_p$ and $\mathbb{C}_p$ are not local fields because the valuation is not discrete [Cre19, p. 25].

[55] Let R be a complete discrete valuation ring with the field of fractions K, L be a finite separable extension of K (also a complete discrete valuation field), and S be the integral closure of R in L. If the unique nonzero prime ideal of the valuation ring S of L is unramified over K, we say that L is an unramified extension of K [KKS11, Proposition 6.54] [Voi21, Definition 13.2.3]. In particular, if K is a complete discrete valuation field whose residue field k is a finite field, then for all $f \in \mathbb{Z}_{\geq 1}$, there is a unique unramified extension $K^{un,f}$ of K of degree f and such a field corresponds to the unique extension of the residue field k of degree f [KKS11, Corollary 6.55] [Voi21, Rem 13.2.5].

[56] $\mathbb{Q}_p$ has a unique unramified extension of degree f for each f, obtained as the splitting field of $x^{p^f} - x$, i.e. by adjoining the $p^f - 1$th roots of unity. It is common to write $K^{un,f} = \mathbb{Q}_{p^f}$ for $K = \mathbb{Q}_p$ since the residue field of $K^{un,f}$ here is $\mathbb{F}_{p^f}$ [Neu99, Proposition II.7.12].

[57] They are fields whose completions are local fields and which satisfy a product formula [Sut17, Lecture 13] [DS12, §4.2].

[58] This is the completion in the sense of Cauchy sequences of K with respect to the valuation corresponding to the place v [Déc98, Definition 1.46] [KKS11, §6.2(d)].

[59] This is the analogue of the fact that the discriminant ideal of a number field extension is divisible by ramifying primes [Neu99, Proposition I.8.4, Corollary III.2.12].

5.4, 6.16]. If $\operatorname{char} K = 2$, then a quadratic K-algebra A is separable if and only if $A \cong K[T]/\langle T^2 + T + a\rangle$ for some $a \in K$. That is, if we let $A = K[i] \cong K[T]/\langle T^2 + T + a\rangle$, then $(A, b \mid K) \cong [a, b \mid K)$, where

$$[a, b \mid K) := \langle i, j \mid i^2 + i = a, j^2 = b, ij = j(i + 1)\rangle$$

for $a \in K$ and $b \in K^\times$ [Voi13, Eq. 1.11] [GS17, Remark 1.1.8] [Voi21, Definition 6.2.1, Theorem 6.4.11]. For example, $[1, 1 \mid K) \cong M_2(K)$ [Voi21, Example 6.2.3]. Moreover, B has a unique standard involution given by

$$\begin{aligned} \overline{} : B &\to B \\ \alpha := t + xi + yj + zij &\mapsto (t + x) + xi + yj + zij := x + \alpha \end{aligned}$$

On the other hand, if $\operatorname{char} K \neq 2$, then a quadratic K-algebra A is separable if and only if $A \cong K[T]/\langle T^2 - a\rangle$ for some $a \in K^\times$. That is, if we let $A = K[i] \cong K[T]/\langle T^2 - a\rangle$, then $(A, b \mid K) \cong (a, b \mid K)$, where

$$(a, b \mid K) := \langle i, j \mid i^2 = a, j^2 = b, ij = -ji\rangle$$

for $a, b \in K^\times$ [Voi13, Eq. 1.10] [GS17, Definition 1.1.1, Lemma 1.2.2] [Cla05, Lec 4, Prop 3] [Voi21, Proposition 2.3.1, Main Theorem 5.4.4]. For example, $\mathbb{H} \cong (-1, -1 \mid \mathbb{R})$ and $(1, b \mid K) \cong (1, 1 \mid K) \cong M_2(K)$ [Voi21, Examples 2.2.3, 2.2.4, Corollary 2.3.6]. Moreover, B has a unique standard involution given by

$$\begin{aligned} \overline{} : B &\to B \\ \alpha := t + xi + yj + zij &\mapsto t - xi - yj - zij \end{aligned}$$

We call the set $\{1, i, j, ij\}$ a quaternion basis of B. Consequently, we can define a *reduced trace* and *reduced norm* on B as [Voi21, Definition 3.3.9]

$$\begin{aligned} \operatorname{trd} : B &\to K \\ \alpha &\mapsto \alpha + \overline{\alpha} \end{aligned} \qquad\qquad \begin{aligned} \operatorname{nrd} : B &\to K \\ \alpha &\to \alpha\overline{\alpha} \end{aligned}$$

The maps trd and nrd are reduced with respect to algebra trace and norm, respectively [Voi21, Remark 3.3.8]. That is, $\operatorname{Tr}_{B/K}(\alpha) = 2\operatorname{trd}(\alpha)$ and $\operatorname{Nm}_{B/K}(\alpha) = \operatorname{nrd}(\alpha)^2$ [Voi21, ¶16.4.8]. In particular, if $B = M_2(K)$ then $\operatorname{trd}(\alpha) = \operatorname{tr}(\alpha)$ and $\operatorname{nrd}(\alpha) = \det(\alpha)$. Observe that, trd is K-linear and nrd is multiplicative. Moreover, we can define K-subspace $B^0 \subseteq B$ and the subgroup $B^1 \leq B^\times$ as [Voi21, Eq. 3.3.5]

$$B^0 := \{\alpha \in B \mid \operatorname{trd}(\alpha) = 0\} \qquad\qquad B^1 := \{\alpha \in B^\times \mid \operatorname{nrd}(\alpha) = 1\}$$

However, $[a, b \mid K)$ is not symmetric in a, b, whereas $(a, b \mid K) \cong (b, a \mid K)$ is symmetric [Voi21, §2.2, 6.2, Exercises 2.4, 6.6]. Furthermore, for $\operatorname{char} K \neq 2$, we can perform computations using SageMath:

```
sage: B.<i,j,k> = QuaternionAlgebra(-1,-23) #k=ij
sage: B
Quaternion Algebra (-1, -23) with base ring Rational Field
sage: B.basis()
(1, i, j, k)
sage: B.is_division_algebra()
True
sage: B.discriminant() #principal ideal generated by product of ramified primes
23
sage: B.ramified_primes() #definite quaternion algebra
[23]
sage: alpha = 1/2 + 2/3*i - 3/4*j + 5/7*k
sage: alpha.conjugate() #standard involution
1/2 - 2/3*i + 3/4*j - 5/7*k
sage: alpha.reduced_trace()
1
sage: alpha.reduced_norm()
178987/7056
```

We will end our discussion with explicit presentations of *definite* quaternion algebras $B_{p,\infty}$ over $\mathbb{Q}$ with $\operatorname{disc}(B_{p,\infty}) = p$, i.e. $\operatorname{Ram}(B_{p,\infty}) = \{p, \infty\}$ [Piz80, Proposition 5.1] [PL17, Proposition 1] [Eis+18, Proposition 1] [Voi21, Example 14.2.13]

1. if $p = 2$ then $B_{p,\infty} = (-1, -1 \mid \mathbb{Q})$;
2. if $p \equiv 3 \pmod 4$ then $B_{p,\infty} = (-1, -p \mid \mathbb{Q})$; and
3. if $p \equiv 1 \pmod 4$ then $B_{p,\infty} = (-\ell, -p \mid \mathbb{Q})$ where $\ell \equiv 3 \pmod 4$ is a prime such that $\left(\frac{\ell}{p}\right) = -1$. In particular,
   (a) if $p \equiv 5 \pmod 8$ then $B_{p,\infty} = (-2, -p \mid \mathbb{Q})$; and
   (b) if $p \equiv 1 \pmod 8$ then $B_{p.\infty} = (-\ell, -p \mid \mathbb{Q})$ where $\ell \equiv 3 \pmod 4$ is a prime such that $\left(\frac{\ell}{p}\right) = -1$.

Explicit presentations of *indefinite* quaternion algebras over $\mathbb{Q}$ with specified discriminant are also known [AB04, Proposition 1.25, Table A.2, A.3]. We can also use SageMath to get these quaternion algebras from the discriminant:

```
sage: B == QuaternionAlgebra(23) #23 = 3 mod 4
True
sage: QuaternionAlgebra(5)
Quaternion Algebra (-2, -5) with base ring Rational Field
sage: QuaternionAlgebra(-3,-5) == QuaternionAlgebra(5)
False
sage: QuaternionAlgebra(-3,-5).discriminant()
5
```

1.2.2 Quaternion orders

Let R be a Dedekind domain[60], $K = \operatorname{Frac} R$ its field of fractions[61] and B be a quaternion K-algebra.

A *quaternion order*[62] O is an R-algebra[63] that is finitely-generated torsion free R-module with $B = O \otimes_R K$ [Voi13, p. 260] [Voi21, ¶10.2.2]. When we want to specify R we may say "R-order in B" [Mar17, p. 114]. Equivalently, $O \subseteq B$ is an R-order iff O is a ring whose elements are integral[64], contains R and $O \otimes_R K = B$ [Déc98, Lemma 1.18] [AB04, Proposition 1.30] [Voi21, Lemma 10.3.7]. However, the set of all integral elements need not form an order. For example, for $B = M_2(\mathbb{Q})$ we can find integral elements $\alpha, \beta \in B$ such that neither $\alpha + \beta$ nor $\alpha\beta$ are integral [Déc98, pp. 9–10] [Cla05, Lec 9, Example 1] [Mar17, Example 4.1.2] [Voi21, Example 10.1.1]. If $O, O' \subseteq B$ are $R-$orders, then O, O' are said to be of the same type if they are isomorphic as R-algebras [Voi21, Lemma 17.4.2]. Equivalently, R-orders O, O' are of the same type iff there exists $\alpha \in B^\times$ such that $O' = \alpha^{-1} O \alpha$ [Voi21, Definition 17.4.1]. The *type set* $\operatorname{Typ}(O)$ of

[60] In general, we can work with noetherian domains, as in [Rei03, Chapter 2] [Voi13, §1] [Voi21, Chapters 9, 10]. However, we are primarily concerned with projective R-modules and if R is a Dedekind domain, then a finitely generated torsion free R-module is automatically projective [Cla15, Corollary 7.24, Theorem 20.15].

[61] Every field of characteristic zero is the field of fractions of some integral domain which is not a field, like $\mathbb{Q} = \operatorname{Frac}\mathbb{Z} = \operatorname{Frac}\mathbb{Z}[1/2] = \operatorname{Frac}\mathbb{Z}[a/b]$, $\mathbb{Q}(\sqrt{d}) = \operatorname{Frac}\mathbb{Z}[\sqrt{d}]$, and $\mathbb{Q}_p = \operatorname{Frac}\mathbb{Z}_p$. In general, if K is a field of characteristic zero with a transcendence basis (X_i) over $\mathbb{Q}$ then $K = \operatorname{Frac} R$ where R is the integral closure of $\mathbb{Z}[\{X_i\}]$ in K ($R \neq K$ since integral extensions preserve dimension), see `https://math.stackexchange.com/a/497287/`. In particular, algebraic number field is the field of fractions of its ring of integers (Dedekind domains), see `https://math.stackexchange.com/a/291679`. Moreover, $\mathbb{C}$ is isomorphic to the field of fractions of the integral closure of $\mathbb{C}[t]$ in the algebraic closure of its field of fractions, see `https://math.stackexchange.com/a/415248/`. It is also possible to realize $\mathbb{R}$ as a field of fractions, see `https://mathoverflow.net/q/67704/`. On the other hand, a field of characteristic $p > 0$ is the field of fractions of some integral domain which is not a field if and only if it is not an algebraic extension of its prime field, see `https://math.stackexchange.com/a/4769641/`.

[62] It is the analogue of an *order* of a number field [Neu99, Definition I.12.1]. Not to be confused with the *order theory* language [Cla15, §2.1].

[63] An R-algebra O is an associative ring with 1 equipped with an embedding $R \hookrightarrow O$ of rings (taking $1 \in R$ to $1 \in O$) whose image lies in the center of O; we identify R with its image under this embedding.

[64] Here, $\alpha \in B$ is integral over R if and only if $\operatorname{trd}(\alpha), \operatorname{nrd}(\alpha) \in R$ [Déc98, Lemma 1.16] [Voi21, Corollary 10.3.6].

O is the set of isomorphism classes of orders. Furthermore, the *genus* $\mathrm{Gen}(O)$ of O is the set of R-orders in B locally isomorphic to O [Voi21, Definition 17.4.5, 17.4.8].

We define the *reduced discriminant*[65] $\mathrm{discrd}(O) := \mathrm{nrd}(\mathrm{diff}(O))$, where

$$\begin{aligned}\mathrm{diff}(O) &:= \mathrm{codiff}(O)^{-1} = \{\alpha \in B \mid \mathrm{codiff}(O)\alpha\,\mathrm{codiff}(O) \subseteq \mathrm{codiff}(O)\}; \text{and}\\ \mathrm{codiff}(O) &:= \{\alpha \in B \mid \mathrm{trd}(\alpha O) \subseteq R\}\end{aligned}$$

i.e. $\mathrm{discrd}(O)$ is the reduced norm[66] of $\mathrm{diff}(O)$ [AB04, Definition 1.31] [Cla05, Lec 9, §1.1] [Mar17, §6.1] [Voi21, ¶16.8.3]. The orders in a genus have a common reduced discriminant, because the reduced discriminant is well-behaved under automorphisms [Voi21, ¶17.4.9]. When working over $R = \mathbb{Z}$, it is common to take the discriminant instead to be the positive generator of the discriminant as an ideal [Voi21, Remark 15.2.4]. Moreover, if we have R-orders $O \supseteq O'$ then $\mathrm{discrd}(O) \supseteq \mathrm{discrd}(O')$ with $O = O'$ iff $\mathrm{discrd}(O) = \mathrm{discrd}(O')$ [AB04, Proposition 1.32] [Cla05, Lec 9, Proposition 5] [Mar17, Proposition 6.1.3] [Voi21, Lemma 15.5.1].

Therefore, there exists a *maximal R-order* $O \subseteq B$ and we can use the reduced discriminant to detect when orders are maximal [Rei03, Corollary 10.4] [Voi21, Proposition 15.5.2]. Moreover, there is a unique genus of maximal R-orders in a quaternion algebra B, i.e. every two maximal orders are locally isomorphic [Voi21, ¶17.4.10]. If K is a nonarchimedean local field, R is its valuation ring and $B \cong (K^{un,2}, \varpi \mid K)$ is the division algebra, then B has a unique maximal order $O \cong S \oplus Sj$ where S is the valuation ring of $K^{un,2}$, with $\mathrm{discrd}(O) = \varpi R$ [AB04, Lemma 1.45] [Mar17, Theorem 4.3.2] [Voi21, Proposition 13.3.4, Theorem 13.3.11, ¶15.2.12]. On the other hand, if K is a local field with $B \cong M_2(K)$ split, then every maximal R-order O is conjugate in B to $M_2(R)$ with $\mathrm{discrd}(O) = R$ [AB04, Lemma 1.46] [Mar17, Theorem 4.2.7] [Voi21, Corollary 10.5.5, ¶23.2.3]. Moreover, if K is a global field then O is a maximal order iff $\mathrm{discrd}(O) = \mathrm{disc}(B)$ [Piz80, Proposition 1.1] [Koh96, Proposition 42] [AB04, Proposition 1.50] [Mar17, Corollary 6.1.14] [Voi21, Theorem 15.5.5]. We can use this for computing maximal orders of quaternion algebras when K is a number field [Voi13, §7]. For example, for quaternion algebras $B_{p,\infty}$ over $\mathbb{Q}$ we know following explicit examples of maximal orders [Has80, Proposition 4] [Piz80, Proposition 5.2] [Koh+14, Lemma 2, 3, 4] [Mar17, Theorem 6.1.15] [PL17, Proposition 1] [Eis+18, Proposition 1] [Voi21, Example 15.5.7]

1. if $p = 2$ then $O = \mathbb{Z}\left\langle 1, i, j, \dfrac{1+i+j+k}{2}\right\rangle$ for $i^2 = j^2 = -1$ and $k = ij$;

2. if $p \equiv 3 \pmod 4$ then $O = \mathbb{Z}\left\langle 1, i, \dfrac{1+j}{2}, \dfrac{i+k}{2}\right\rangle$ for $i^2 = -1$, $j^2 = -p$ and $k = ij$; and

3. if $p \equiv 1 \pmod 4$ then $O = \mathbb{Z}\left\langle 1, \dfrac{1+j}{2}, \dfrac{i+k}{2}, \dfrac{cj+k}{\ell}\right\rangle$ for $c \in \mathbb{Z}$ such that $c^2 \equiv -p \pmod \ell$, $i^2 = -\ell$, $j^2 = -p$ and $k = ij$, where $\ell \equiv 3 \pmod 4$ is a prime such that $\left(\dfrac{\ell}{p}\right) = -1$. In particular,

    (a) if $p \equiv 5 \pmod 8$ then $O = \mathbb{Z}\left\langle 1, i, \dfrac{1+j+k}{2}, \dfrac{1+2j+k}{4}\right\rangle$ for $i^2 = -2$, $j^2 = -p$ and $k = ij$; and

    (b) if $p \equiv 1 \pmod 8$ then $O = \mathbb{Z}\left\langle 1, \dfrac{1+i}{2}, j, \dfrac{ci+k}{\ell}\right\rangle$ for $c \in \mathbb{Z}$ such that $c^2 \equiv -p \pmod \ell$, $i^2 = -\ell, j^2 = -p$ and $k = ij$, where $\ell \equiv 3 \pmod 4$ is a prime such that $\left(\dfrac{\ell}{p}\right) = -1$.

[65] It is the analogue of the fact that the discriminant ideal of a Dedekind domain is obtained by taking norm of the different ideal [Neu99, Theorem III.2.9]. Equivalently, we can define $\mathrm{discrd}(O)$ as the square-root of the ideal generated by $\{\det(\mathrm{trd}(\alpha_i\alpha_j)_{1\le i,j\le 4}) \mid \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in O\}$ [KV10, p. 1718] [Voi13, p. 287] [Voi21, Lemma 15.4.7] [Col22, p. 163]. There also exist slight variations of this like defining $\mathrm{discrd}(O)$ as the square-root of the ideal generated by $\{\det(\mathrm{trd}(\alpha_i\overline{\alpha_j})_{1\le i,j\le 4}) \mid \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in O\}$ [Brz83, p. 503] [Koh96, p. 65] [Lem11b, pp. 7–8] or $\left\{\det\left(\dfrac{1}{2}\,\mathrm{trd}(\alpha_i\overline{\alpha_j})_{1\le i,j\le 4}\right) : \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in O\right\}$ [Ler22, p. 26] [Ver23, p. 27].

[66] This is the R-submodule of K, generated by the set $\{\mathrm{nrd}(\alpha) \mid \alpha \in \mathrm{diff}(O)\}$ [Voi21, Definition 16.3.1]. When working over $R = \mathbb{Z}$, it is common to take the reduced norm instead to be the positive generator $\gcd(\{\mathrm{nrd}(\alpha) \mid \alpha \in \mathrm{diff}(O)\})$ of the fractional ideal of $\mathbb{Q}$ [Voi21, p. 259].

Further results on explicit constructions of maximal orders for definite quaternion algebras over $\mathbb{Q}$ are given in [Ibu82]. Moreover, we can study the $\mathbb{Z}$-orders using SageMath:

```
sage: O = B.quaternion_order([1, i, (1+j)/2, (i+k)/2]) #ZZ-order
sage: O
Order of Quaternion Algebra (-1, -23) with base ring Rational Field with basis
    (1, i, 1/2 + 1/2*j, 1/2*i + 1/2*k)
sage: O.discriminant() #discrd(O); a maximal order
23
sage: O == B.maximal_order() #same as the explicit maximal order in database
True
```

An *Eichler order*[67] $O \subset B$ is the intersection of two (not necessarily distinct) maximal orders [Déc98, Definition 1.24] [AB04, Definition 1.34] [Cla05, Lec 9, p. 1] [KV10, p. 1718] [Mar17, Example 4.2.7] [Voi21, Definition 23.4.1]. If K is a nonarchimedean local field and B is a division algebra, then the maximal order is the unique Eichler R-order in B [AB04, Lemma 1.45]. On the other hand, if K is a local field with $B \cong M_2(K)$ split, then every Eichler R-order O is the intersection of a uniquely determined pair of maximal orders (not necessarily distinct) [AB04, Proposition 1.47(d)] [Voi21, Proposition 23.4.3(iv)]. Equivalently, a local Eichler order $O \subseteq M_2(K)$ is conjugate to a *standard Eichler order of level* $\mathfrak{p}^e$

$$O_0(\mathfrak{p}^e) \coloneqq \begin{pmatrix} R & R \\ \mathfrak{p}^e & R \end{pmatrix}$$

where $e \geq 0$ and $\mathfrak{p} = \varpi R$ is the maximal ideal of the complete discrete valuation ring R [AB04, Proposition 1.47(c)] [Voi21, Definition 23.4.11]. In general, if O is a local Eichler order, then the *level*[68] of O is the ideal

$$\operatorname{lev}(O) \coloneqq \begin{cases} R & \text{if } B \text{ is a division algebra} \\ \mathfrak{p}^e & \text{if } B \text{ is split with } O \cong O_0(\mathfrak{p}^e) \end{cases}$$

where $\operatorname{discrd}(O) = \operatorname{lev}(O)$ for local Eichler order $O \subseteq M_2(K)$ [AB04, Definition 1.48] [Mar17, Proposition 6.1.8] [Voi21, ¶23.4.12]. Moreover, by the local-global dictionary for orders, the property of being an Eichler order is local [AB04, Proposition 1.51] [Mar17, Proposition 6.1.10] [Voi21, Lemma 9.5.3, Lemma 10.4.3]. That is, if K is a global field then the level of a global Eichler order O is the unique ideal in R

$$\operatorname{lev}(O) \coloneqq \prod_{\substack{v \in \operatorname{Pl}(K) \\ v \text{ finite}}} \operatorname{lev}(O_v)$$

where $O_v = O \otimes_R R_v$ and R_v is the complete discrete valuation ring of local field K_v [AB04, Definition 1.52]. That is, if O is a global Eichler order, then $\operatorname{discrd}(O) = \operatorname{disc}(B)\operatorname{lev}(O)$ where $\operatorname{disc}(B)$ and $\operatorname{lev}(O)$ are co-prime ideals in R [AB04, Proposition 1.53, Proposition 1.54(i)] [Voi21, ¶23.4.19]. If $K = \mathbb{Q}$, $N \in \mathbb{Z}_{>0}$, and $O \subset B$ an Eichler order of level $N\mathbb{Z}$, then we simply say $\operatorname{lev}(O) = N$; i.e. the maximal orders are the Eichler orders of level 1 [Mar17, Definition 6.1.11] [Ler22, p. 27]. In particular, if O is an order in quaternion $\mathbb{Q}$-algebra with $\operatorname{discrd}(O) = \operatorname{disc}(B)N$ a square-free integer, then O is an Eichler order of level N [AB04, Proposition 1.54(ii)]. Furthermore, if B is a quaternion $\mathbb{Q}$-algebra, then for each integer N such that $\gcd(\operatorname{disc}(B), N) = 1$, there exist Eichler orders of level N [Déc98, Theorem 1.58] [AB04, Corollary 1.58]. Explicit construction of Eichler orders in quaternion $\mathbb{Q}$-algebras can be found in [Has95, §2] and [AB04, §1.2.4, Tables A.4–A.7]. Moreover, the *Bruhat-Tits tree*[69] provides a visual way to keep track of many calculations with Eichler orders [Tit79] [Cla05, Lec 9, p. 5] [Yu09] [FM14, §2.2] [Gul20, Day 2 Lecture

[67] Martin Eichler wrote his dissertation with Heinrich Brandt on quaternion algebras and later worked on more general types of simple algebras. Eichler famously illustrated connections of quaternion algebras with other mathematical subjects using a hexagon with its vertices labeled clockwise as follows: automorphic forms, modular forms, quadratic forms, quaternion algebras, Riemann surfaces, and algebraic functions [Cou96, p. 1344] [Mar17, pp. 5–6].

[68] It is possible to define *level* for all quaternion orders over local and global fields of characteristic zero, as done in [Mar17, Definition 6.1.6, Corollary 6.1.9, Definition 6.1.11, Corollary 6.1.13]. Another generalization for orders in $B_{p,\infty}$ is given in [Piz80, Definition 1.2] and [Déc98, Definition 1.57].

[69] A nice tool for illustrations: `https://github.com/ariymarkowitz/Bruhat-Tits-Tree-Visualiser`

notes] [Voi21, ¶23.5.16, Exercise 23.10] [Amo+21, §2.3]. For example, we can use SageMath to verify that $\mathbb{Z}\left\langle 1, i, j, \dfrac{1+i+j+k}{2}\right\rangle$ is an Eichler order of level 2 in $B_{23,\infty}$:

```
sage: OO = B.quaternion_order([1,i, (i+j)/2, (1+k)/2])
sage: OO == O
False
sage: OO.discriminant() #another maximal order, [Koh+14, Lemma 2]
23
sage: OE = O.intersection(OO) #Eichler order
sage: OE
Order of Quaternion Algebra (-1, -23) with base ring Rational Field with basis
    (1/2 + 1/2*i + 1/2*j + 1/2*k, i, j, k)
sage: OE == B.quaternion_order([1,i,j,(1+i+j+k)/2])
True
sage: OE.discriminant()/B.discriminant() #level of global Eichler order
2
```

There are many other categories of quaternion orders. For example, hereditary, Gorenstein and Bass orders are discussed in [Brz83], [Lem11b] and [Voi21, Chapter 24].

A *quaternion fractional ideal*[70] I over R is a finitely generated torsion free R-module such that $B = I \otimes_R K$ [De +20, §2.2] [Eri+23, §2.4]. When we want to specify R we may say "fractional R-ideal in B." In other words, a fractional R-ideal in B that is a subring is called R-order in B. The reduced norm $\mathrm{nrd}(I)$, of a fractional R-ideal I in B, is a fractional ideal of K, i.e., $\mathrm{nrd}(I)$ is finitely generated as a R-submodule of K [Déc98, Definition 1.26] [Voi21, Lemma 16.3.2]. Moreover, given a fractional R-ideal I in B, we define the *left order of* I and *right order of* I as

$$O_{\mathsf{L}}(I) \coloneqq \{\alpha \in B \mid \alpha I \subseteq I\} \qquad\qquad O_{\mathsf{R}}(I) \coloneqq \{\alpha \in B \mid I\alpha \subseteq I\}$$

respectively, such that both are R-orders in B [Piz80, Definition 1.14] [Déc98, Definition 1.25] [Mar17, Proposition 4.2.8] [Voi21, Lemma 10.2.7]. Furthermore, for $R = \mathbb{Z}$, we can use SageMath to study these:

```
sage: I = B.ideal([1,i,j,2*k]) #fractional ZZ-ideal; not ZZ-order, nrd(I) != 1
sage: I
Fractional ideal (1, i, j, 2*k)
sage: I.norm() #reduced norm; the generator of fractional ideal of QQ
1/2
sage: OLI = I.left_order()
sage: OLI
Order of Quaternion Algebra (-1, -23) with base ring Rational Field with basis
    (1, 2*i, 2*j, 2*k)
sage: ORI = I.right_order()
sage: ORI
Order of Quaternion Algebra (-1, -23) with base ring Rational Field with basis
    (1, 2*i, 2*j, 2*k)
sage: OLI.discriminant() #not maximal
736
```

A fractional R-ideal I in B is said to be *principal* if there exists $\alpha \in B$ such that $I = O_{\mathsf{L}}(I)\alpha = \alpha O_{\mathsf{R}}(I)$;

[70] It is the analogue of a *fractional ideal* of the field of fractions of a Dedekind domain [Neu99, Definition I.3.7]. Not to be confused with an ideal in B, i.e. a two-sided ideal in the associative ring B which can only be either $\langle 0\rangle$ or B because B is a simple algebra. This is also referred by different terms like *ideal* [Déc98, Definition 1.14] [AB04, Definition 1.28] [Cla05, Lec 9, p. 1] [Sil21, p. 33] [Amo+21, §2.2.1], *complete lattice* [Rei03, pp. 44, 108] [Mar17, p. 114], and *lattice* [Piz80, p. 343] [Brz83, p. 503] [Koh96, p. 58] [KV10, p. 1717] [Eis+18, §2.2] [Eis+20, §2B] [Ler22, Definition 1.2.6] [Arp22, Definition 1.5.1] [Col22, p. 163] [Ver23, Definition 2.3.6]. I find the abuse of term "lattice" to refer these quite confusing, because *lattice* itself has two other definitions, one in geometry of numbers [Sie89] [Neu99, Definition I.4.1] [HPS14, Theorem 7.17] [Sma16, §5.1.3] [Voi21, Definition 17.5.1] and other in order theory [Cla15, §2.2]. Moreover, the notation for R-lattices is switched from "M" in chapter 9 to "I" in chapter 10 onwards in [Voi21, Definition 9.3.1, ¶10.2.5]. However, once can justify the usage of term "lattice" by studying *quaternion orders* as an analogue of *quadratic orders* [Gul20] [Voi21, §16.1] [Ler22, §1.2.2] [Cox22, Theorem 10.14] [Ver23, pp. 22–23].

we say that I is generated by α [Voi21, Definition 16.2.1]. Moreover, since $I \otimes_R K = B$, we have $\alpha \in B^\times$ and $O_{\mathsf{R}}(I) = \alpha^{-1} O_{\mathsf{L}}(I)\alpha$ [Voi21, ¶16.2.2, 16.2.3].

Let I and J be fractional R-ideals in B, then the *product* IJ is defined to be the R-submodule of B generated[71] by the set $\{\alpha\beta \mid \alpha \in I, \beta \in J\}$; i.e. the product IJ is a fractional R-ideal [Voi21, p. 260]. We say that the product IJ is *compatible*[72] to mean that $O_{\mathsf{R}}(I) = O_{\mathsf{L}}(J)$; this relation is neither symmetric nor transitive [Voi21, Definition 16.2.5]. That is, the compatible product IJ can be thought of as a special case of the tensor product of modules [Voi21, Remark 16.2.6]. For $R = \mathbb{Z}$, we can use SageMath to compute these ideal products:

```
sage: J = B.ideal([(1+j)/2, (i + 3*k)/2, 2*j, 2*k]) #another fractional ZZ-ideal
sage: J
Fractional ideal (1/2 + 1/2*j, 1/2*i + 3/2*k, 2*j, 2*k)
sage: OLJ = J.left_order()
sage: OLJ
Order of Quaternion Algebra (-1, -23) with base ring Rational Field with basis
    (1/2 + 1/2*j, 1/4*i + 3/4*k, j, 2*k)
sage: ORJ = J.right_order()
sage: ORJ
Order of Quaternion Algebra (-1, -23) with base ring Rational Field with basis
    (1/2 + 1/2*j, 1/2*i + 1/2*k, j, k)
sage: I*J
Fractional ideal (1/2 + 1/2*j, 1/2*i + 1/2*k, j, k)
sage: ORI == OLJ #IJ not compatible
False
```

A fractional R-ideal I in B is *invertible* if there exists a fractional R-ideal I' in B that is a (two-sided) inverse to I, i.e. $II' = O_{\mathsf{L}}(I) = O_{\mathsf{R}}(I')$ and $I'I = O_{\mathsf{L}}(I') = O_{\mathsf{R}}(I)$ [Voi21, Definition 16.5.1]. For example, if $I = O_{\mathsf{L}}(I)\alpha$ is principal, then I is invertible with $I' = \alpha^{-1}O_{\mathsf{L}}(I)$ [Voi21, ¶16.5.4]. Moreover, I is invertible if and only if $I^{-1} \coloneqq \{\alpha \in B \mid I\alpha I \subseteq I\}$ is a (two-sided) inverse for I [Déc98, Definition 1.28] [Voi21, Proposition 16.5.8]. For example, if O is an R-order then $O^{-1} = O$. If IJ is a compatible product of invertible ideals, then (1) IJ is also invertible [Voi21, ¶16.5.3]; (2) $O_{\mathsf{L}}(IJ) = O_{\mathsf{L}}(I)$ and $O_{\mathsf{R}}(IJ) = O_{\mathsf{R}}(J)$ [Voi21, Lemma 16.5.11]; and (3) $\operatorname{nrd}(IJ) = \operatorname{nrd}(I)\operatorname{nrd}(J)$ [Voi21, ¶16.6.13]. A fractional R-ideal I is an R-order if and only if $1 \in I$, every element of I is integral, and I is invertible [Voi21, Corollary 16.6.12]. The set of invertible fractional R-ideals in B is a groupoid[73] under inverse and compatible product; the R-orders in B are the identity elements in this groupoid [Voi21, Proposition 19.4.1]. The subset of invertible fractional R-ideals whose (left or) right order belong to a specified genus of orders $\operatorname{Gen}(O)$ is a connected[74] subgroupoid, called *Brandt groupoid*[75] of the genus of O [Voi21, Definition 19.4.3]

$$\operatorname{Brt}(O) \coloneqq \{I \mid I \subset B \text{ invertible fractional } R\text{-ideal and } O_{\mathsf{L}}(I), O_{\mathsf{R}}(I) \in \operatorname{Gen}(O)\}$$

Furthermore, if either $O_{\mathsf{L}}(I)$ or $O_{\mathsf{R}}(I)$ is maximal, then I is invertible, and both $O_{\mathsf{L}}(I)$ and $O_{\mathsf{R}}(I)$ are also maximal [Rei03, Theorem 23.10] [Voi21, Proposition 16.6.15(b), Theorem 18.1.2(a), Proposition 18.3.2]. We call a fractional R-ideal I a *normal ideal* if both $O_{\mathsf{L}}(I)$ and $O_{\mathsf{R}}(I)$ are maximal orders [Déc98, Definition 1.27] [Rei03, p. 193]. For $R = \mathbb{Z}$, we can use reduced discriminant in SageMath to check if the left(right)-order is maximal:

```
sage: OLJ.discriminant() #maximal; J is invertible
23
```

[71] This definition is the same as for ideals in a commutative ring: https://math.stackexchange.com/q/290229

[72] Some authors call such multiplication to be *proper* [Rei03, pp. 183, 196] [Mar17, p. 127].

[73] The group is the set of isomorphisms in a groupoid, endowed with the operation of composition of morphisms [Alu09, §II.1.1].

[74] Viewing the groupoid as a small category, we say two objects are connected if there exists a morphism between them, and the category is connected if every two objects are connected [Voi21, ¶19.3.8].

[75] In 1927, Heinrich Brandt introduced a class of partial binary algebraic structures and called them *groupoids*. This was long before the notion of *category* was formulated. Contemporary notion of a *connected groupoid* is equivalent to a Brandt groupoid. Brandt used the notion of a groupoid to extend the ideal class group in rings of algebraic integers to the non-commutative case [HK04, §3.5] [Voi21, Remark 19.3.12].

```
sage: ORJ.discriminant() #also maximal; J is normal
23
```

The *involution* of a fractional R-ideal in B is given by $\overline{I} := \{\overline{\alpha} \mid \alpha \in I\}$, where $\overline{\ \ }$ is the standard involution of B; $\overline{I}$ is a fractional R-ideal in B [Voi21, ¶16.6.6]. This has properties like, (1) $\overline{IJ} = \overline{J}\,\overline{I}$ (even if this product is not compatible); (2) $O_{\mathsf{L}}(\overline{I}) = O_{\mathsf{R}}(I)$ and $O_{\mathsf{R}}(\overline{I}) = O_{\mathsf{L}}(I)$ [Voi21, Lemma 16.6.7]. Moreover, if I is invertible, then $I^{-1} = \overline{I}\,\mathrm{nrd}(I)^{-1}$, where $\mathrm{nrd}(I)$ is an invertible fractional ideal of K since R is a Dedekind domain [Neu99, Proposition I.3.8] [Voi21, ¶16.6.14]. For example, we can use SageMath to find inverse of the invertible fractional R-ideal J from above:

```
sage: Jbar = J.conjugate() #involution ideal
sage: Jbar
Fractional ideal (1/2 + 3/2*j, 1/2*i + 3/2*k, 2*j, 2*k)
sage: Jbar.left_order() == ORJ
True
sage: Jbar.right_order() == OLJ
True
sage: J.norm() #reduced norm; generator of integral ideal of QQ
2
sage: Jinv = Jbar.scale(1/J.norm())
sage: Jinv
Fractional ideal (1/4 + 3/4*j, 1/4*i + 3/4*k, j, k)
sage: JJinv = J*Jinv
sage: B.quaternion_order(JJinv.basis()) == OLJ == Jinv.right_order() #inverse
True
sage: JinvJ = Jinv*J
sage: B.quaternion_order(JinvJ.basis()) == ORJ == Jinv.left_order() #inverse
True
```

A *quaternion integral ideal*[76] I is a fractional R-ideal in B such that $I \subseteq O_{\mathsf{L}}(I) \cap O_{\mathsf{R}}(I)$ [Eri+23, p. 6]. That is, if I is an integral R-ideal, then every element of I is integral over R [Voi21, Lemma 16.2.8]. In particular, an order is an integral ideal [Cla05, Lec 9, Exercise 1]. Moreover, for a fractional R-ideal I, there exists nonzero $d \in R$ such that Id is an integral R-ideal, i.e. every fractional R-ideal $I = (Id)/d$ is fractional in the sense that it is obtained from an integral R-ideal with denominator [Voi21, p. 261]. For example, we can use SageMath to get integral $\mathbb{Z}$-ideals:

```
sage: OLJcapORJ = B.ideal(basis(OLJ.intersection(ORJ)))
sage: J == J.intersection(OLJcapORJ) #J is integral
True
sage: I == I.intersection(B.ideal(basis(OLI))) #I NOT integral; OLI=ORI
False
sage: I2 = I.scale(2) #multiply on the right with d=2
sage: OLI2 = I2.left_order()
sage: OLI2
Order of Quaternion Algebra (-1, -23) with base ring Rational Field with basis
    (1, 2*i, 2*j, 2*k)
sage: OLI2 == I2.right_order()
True
sage: I2 == I2.intersection(B.ideal(basis(OLI2))) #I2 is integral
True
```

Given an R-order $O \subseteq B$, a *left fractional O-ideal* is a fractional R-ideal such that[77] $O_{\mathsf{L}}(I) = O$ [KV10,

[76] It is the analogue of *integral ideal* of the field of fractions of a Dedekind domain, i.e. an ideal of the Dedekind domain [Neu99, p. 21]. This is also referred by different name like *integral lattice* [Voi21, Lemma 16.2.8].

[77] Most authors use a more relaxed condition, i.e. $O \subseteq O_{\mathsf{L}}(I)$ [Voi21, Definition 16.2.9] [Amo+21, p. 46] [Sil21, p. 33] [Ver23, Definition 2.3.7] [Eri+23, p. 6], or equivalently $\alpha I \subseteq I$ for all $\alpha \in O$ [Koh96, p. 62] [Rei03, pp. 129, 224] [Bel08, p. 10] [Mar17, p. 124] [Col22, p. 163]. Moreover, some call the O-ideals where equality $O = O_{\mathsf{L}}(I)$ holds to be *sated* [Voi21, Definition 16.2.11, ¶16.5.18] or *proper* [Voi21, Remark 16.5.19] [Cox22, p. 106]. However, all of them are eventually interested in maximal orders, and in that situation all these definitions are the same.

p. 1719] [GPS20, §2.1]. In a similar fashion, we may define *right fractional O-ideals*; however, conjugation $I \mapsto \overline{I}$ gives a bijection between the sets of left and right fractional O-ideals, so when dealing with one-sided fractional ideals, it suffices to work with right fractional ideals [KV10, p. 1719] [Voi21, ¶17.3.2]. We say I is a two-sided fractional O-ideal if $O_{\mathsf{L}}(I) = O_{\mathsf{R}}(I) = O$ [Déc98, Definition 1.27] [KV10, p. 1719] [Voi21, ¶18.2.9] [Ver23, p. 27]. For example, $\operatorname{codiff}(O)$ is a two-sided fractional O-ideal [Voi21, Lemma 15.6.16, Example 16.2.12] Moreover, a *left integral O-ideal* is a left ideal of $O_{\mathsf{L}}(I)$ in the usual sense [KV10, p. 1719] [Voi21, Remark 16.2.10, §18.2]. For example, $\operatorname{diff}(O)$ is an integral two-sided O-ideal [Voi21, Lemma 16.8.2]. We can use SageMath[78] to check if a given fractional $\mathbb{Z}$-ideal is some kind of O-ideal:

```
sage: O == OLI #==ORI; I is NOT a left/right fractional O-ideal
False
sage: O == OLJ #J is NOT left fractional O-ideal
False
sage: O == ORJ #J is a right fractional O-ideal; integral because O is maximal
True
```

Let $O, O' \subseteq B$ be R-orders. Then a *fractional O, O'-ideal* is a fractional R-ideal I that is a left fractional O-ideal and a right fractional O'-ideal, i.e. $O_{\mathsf{L}}(I) = O$ and $O_{\mathsf{R}}(I) = O'$ [KV10, p. 1719]. Furthermore, if the fractional O, O'-ideal I is invertible, then I is called the *connecting ideal* and the orders O and O' are said to be connected[79] [KV10, p. 1720] [Ler22, Definition 1.2.16] [Ver23, p. 28] [Eri+23, p. 6]. Equivalently, O is connected to O' if there exists a locally principal fractional O, O'-ideal $I \subseteq B$, called a connecting ideal [Voi21, Lemma 16.5.9, Definition 17.4.4] [Ler22, pp. 29–30]. That is, $\operatorname{Gen}(O)$ is made of all the orders connected to O [Voi21, Lemma 17.4.6]. Therefore, given two orders O_1, O_2 in the same genus, there is a connecting ideal $I(O_1, O_2)$ well-defined up to scalar multiplication and multiplication by a two-sided ideal [Ler22, p. 30]. In particular, for $O_1, O_2 \in \operatorname{Gen}(O)$ when O is a maximal order, the connecting ideals are integral and we can define $I(O_1, O_2)$ to be the connecting integral ideal with the smallest norm [Voi21, Exercise 17.4]. Moreover, the relation of being connected is an equivalence relation, and two Eichler orders O, O' are connected if and only if they have the same level N [KV10, p. 1720]. Therefore, an Eichler order of level N is equivalent data to two maximal orders with a connecting ideal[80] of reduced norm N [Koh+14, Lemma 8] [Arp22, Theorem 3.3.5]. In particular, if O_1, O_2 are two maximal orders in $B_{p,\infty}$ then the Eichler order $O_1 \cap O_2 = \mathbb{Z} + I(O_1, O_2)$ [De +20, Proposition 1] [Ler22, Proposition 2.3.1].

The set of invertible two-sided fractional O-ideals B forms a group under multiplication, and the quotient of this group by the (normal) subgroup of principal ideals of R is called the *Picard group*[81] $\operatorname{Pic}_R(O)$ [Voi21, §18.4]. On the other hand, the quotient of the group of invertible two-sided fractional O-ideals by the *normal* subgroup of principal two-sided fractional O-ideals is called the *two-sided ideal class group of O* [KV10, p. 1720] [Voi21, §18.5]. Finally, we can also study the the *Brandt class groupoid* of the genus of O

$$\operatorname{BrtCl}(O) \coloneqq \bigsqcup_{i,j} \{[I] \mid I \text{ is an invertible fractional } R\text{-ideal with } O_{\mathsf{L}}(I) = O_i \text{ and } O_{\mathsf{R}}(I) = O_j\}$$

where $[I]$ is a *homothety class* of fractional O_i, O_j-ideals where I is homothetic to J if there exists $a \in K^\times$ such that $J = aI$ [Voi21, §19.5]. When O is maximal in a quaternion $\mathbb{Q}$-algebra, we defined $\operatorname{Brt}(B) \coloneqq \operatorname{BrtCl}(O)$ to be the *Brandt groupoid of B* [Amo+21, §2.2.2]. Moreover, we can visualize $\operatorname{Brt}(B)$ as a directed multigraph whose vertices are the isomorphism classes of maximal orders of B, and an edge connects two vertices whenever the corresponding maximal orders are connected by an homothety class [Mar17, Figure 4.4.1] [Voi21, Figure 19.2.2] [Amo+21, Fig. 2]. If we only consider ideal classes which admit representatives of a certain prime reduced norm $\ell \nmid \operatorname{disc}(B)$, then we get an *$\ell$-ideal graph* whose vertices are the isomorphism classes of maximal orders in B, and two vertices are connected by an edge if the corresponding maximal orders are connected by an ideal class admitting a representative of reduced norm ℓ [Amo+21, Definition 1, Fig. 3].

[78] Caution: The methods `left_ideal()` or `right_ideal` don't check if the O-ideal I generated must have $O_{\mathsf{L}}(I) = O$ or $O_{\mathsf{R}}(I) = O$; it instead in an ad-hoc way assigns $O_{\mathsf{L}}(I) \coloneqq O$ or $O_{\mathsf{R}}(I) \coloneqq O$. One can check this using the `_compute_order` method: `https://github.com/sagemath/sage/blob/develop/src/sage/algebras/quatalg/quaternion_algebra.py`

[79] Some authors call such orders to be *linked* [Amo+21, p. 46].

[80] In the SQIsign protocol, such ideals as *cyclic ideals* [Ler22, Definition 1.2.13] [Eis+18, Prop 4.3] [Eis+18, Prop 10].

[81] It is the analogue of the *Picard group* of an order in a number field [Neu99, Definition I.12.5].

Let $I, J \subseteq B$ be invertible[82] fractional R-ideals. We say I, J are in the *same right class*, and we write $I \sim_{\mathsf{R}} J$, if there exists $\alpha \in B^{\times}$ such that $\alpha I = J$ [Voi21, Definition 17.3.1]. Throughout, we will work with the right classes, but analogous definitions can be made for the left classes. The relation $\sim_{\mathsf{R}}$ defines an equivalence relation on the set of fractional R-ideals in B, and the right equivalence class of fractional R-ideal I is denoted $[I]_{\mathsf{R}}$. Since every fractional R-ideal in the class $[I]_{\mathsf{R}}$ is invertible, we call the class *invertible*. Moreover, we have $I \sim_{\mathsf{R}} J$ if and only if I and J are isomorphic as right modules over $O_{\mathsf{R}}(I) = O_{\mathsf{R}}(J)$ [Voi21, Lemma 17.3.3]. Therefore, we organize invertible right classes by their right orders. That is, given an R-order O, the *right class set*[83] of O is

$$\begin{aligned}\mathrm{Cls}_{\mathsf{R}}(O) &:= \{[I]_{\mathsf{R}} \mid I \text{ is an invertible fractional } R\text{-ideal with } O_{\mathsf{R}}(I) = O\} \\ &= \{[I]_{\mathsf{R}} \mid I \text{ is an invertible right fractional } O\text{-ideal}\}\end{aligned}$$

The standard involution induces a bijection between $\mathrm{Cls}_{\mathsf{R}}(O)$ and the analogously defined left class set $\mathrm{Cls}_{\mathsf{L}}(O)$. Since B is noncommutative, the ideal class $[IJ]_{\mathsf{R}}$ of two right fractional O-ideals I, J is in general not determined by the ideal classes $[I]_{\mathsf{R}}$ and $[J]_{\mathsf{R}}$, so the set of right ideal classes may not form a group [KV10, p. 1719]. However, the set $\mathrm{Cls}_{\mathsf{R}}(O)$ has a distinguished element $[O]_{\mathsf{R}} \in \mathrm{Cls}_{\mathsf{R}}(O)$, so it has the structure of a *pointed set*[84] [Voi21, ¶17.3.6]. Moreover, if O, O' are connected R-orders, and J is a connecting O, O' ideal then we get the following mutually inverse bijections

$$\begin{aligned}\mathrm{Cls}_{\mathsf{R}}(O) &\xrightarrow{\sim} \mathrm{Cls}_{\mathsf{R}}(O') \\ [I]_{\mathsf{R}} &\mapsto [IJ]_{\mathsf{R}} \\ [I'J^{-1}]_{\mathsf{R}} &\mapsfrom [I']_{\mathsf{R}}\end{aligned}$$

i.e. if $O' \in \mathrm{Gen}(O)$ then $\mathrm{Cls}_{\mathsf{R}}(O) \leftrightarrow \mathrm{Cls}_{\mathsf{R}}(O')$ [Voi21, Lemma 17.4.11, Remark 17.4.12].

Now, let's restrict our attention to then case when K is a global field. If $O \subset B$ is an R-order, then $\mathrm{Cls}_{\mathsf{R}}(O)$ is a finite set; i.e. the *class number* $h = \#\,\mathrm{Cls}_{\mathsf{R}}(O)$ is finite[85] [Rei03, Theorem 26.4] [Mar17, Theorem 4.4.7] [Voi21, Proposition 17.5.6, Main Theorem 17.7.1, Exercise 17.12, Corollary 27.6.20]. Moreover, since there is a surjective map of sets from $\mathrm{Cls}_{\mathsf{R}}(O)$ to $\mathrm{Typ}(O)$, the type set is also finite [Voi21, Lemma 17.4.13, Corollary 27.6.25]. In particular, $\#\,\mathrm{Cls}_{\mathsf{R}}(O)$ is independent of the choice of Eichler order O of a given level [KV10, Proposition 1.6].

Let B be an indefinite quaternion algebra over $\mathbb{Q}$, i.e. $B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R})$ (matrix algebra). If O is an Eichler $\mathbb{Z}$-order then $\#\,\mathrm{Cls}_{\mathsf{R}}(O) = 1$, i.e. every right O-ideal is principal [Voi21, Corollary 17.8.5, Theorem 28.2.11(a)]. Moreover, since $\mathrm{Typ}(O) = 1$, Eichler orders with the same level in indefinite quaternion $\mathbb{Q}$-algebras are also globally conjugate [AB04, Theorem 1.59] [Voi21, Theorem 28.2.11(b)].

On the other hand, let B be a definite quaternion algebra over $\mathbb{Q}$, i.e. $B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$ (division algebra). If O is an Eichler $\mathbb{Z}$-order then

$$\begin{aligned}\#\,\mathrm{Cls}_{\mathsf{R}}(O) = {} & \frac{\varphi(\mathrm{disc}(B))\psi(\mathrm{lev}(O))}{12} && (17)\\ & + \mathbf{1}_{4\nmid \mathrm{discrd}(O)} \left(\frac{1}{4} \prod_{p \mid \mathrm{disc}(B)} \left(1 - \left(\frac{-4}{p}\right)\right) \prod_{p \mid \mathrm{lev}(O)} \left(1 + \left(\frac{-4}{p}\right)\right) \right) && (18)\\ & + \mathbf{1}_{9\nmid \mathrm{discrd}(O)} \left(\frac{1}{3} \prod_{p \mid \mathrm{disc}(B)} \left(1 - \left(\frac{-3}{p}\right)\right) \prod_{p \mid \mathrm{lev}(O)} \left(1 + \left(\frac{-3}{p}\right)\right) \right) && (19)\end{aligned}$$

where φ is Euler totient function, ψ is Dedekind psi function (as in (12)), $\mathbf{1}_A$ is the indicator function[86], and $\left(\frac{\bullet}{*}\right)$ is the Kronecker symbol (as in (7)) [Piz80, Theorem 1.12] [Déc98, Theorem 1.67] [Voi21, Theorem

[82] We can drop this condition, like S_r in [Déc98, Definition 1.60] and $\mathrm{Cl}_r(O) = \mathrm{Frac}_r(O)/\sim$ in [Mar17, pp. 125, 129]. However, we are eventually interested in maximal and Eichler orders, and in that situation all these definitions coincide.

[83] It is the analogue of *class group* $\mathrm{Cl}(R)$ of a Dedekind domain R [Neu99, pp. 22 and 70]. Here we use Cls to emphasize that we are working with a class *set* [Voi21, Remark 17.3.5].

[84] That is, a set equipped with a distinguished element of the set

[85] It is the analogue of the fact that ideal class group $\mathrm{Cl}(O)$ of an algebraic number field K is finite [Neu99, Theorem I.6.3].

[86] The 0-1 indicator function is defined as $\mathbf{1}_A = 1$ if A is true, and $\mathbf{1}_A = 0$ otherwise.

25.1.1, Theorem 25.3.18, Theorem 30.1.5, Remark 30.8.8]. In particular, when O is a maximal $\mathbb{Z}$-order in $B_{p,\infty}$, we get

$$\#\,\mathrm{Cls}_{\mathsf{R}}(O) = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \pmod{12} \\ 1 & \text{if } p = 2,3;\ p \equiv \pm 5 \pmod{12} \\ 2 & \text{if } p \equiv -1 \pmod{12} \end{cases} \tag{20}$$

which is almost same as (13), exactly like (9), hinting towards a relationship between supersingular elliptic curves and maximal $\mathbb{Z}$-orders of $B_{p,\infty}$ [Déc98, Theorem 1.66, Corollary 2.13] [Voi21, ¶42.3.8]. For example, since $O = \mathbb{Z}\left\langle 1, i, \dfrac{1+j}{2}, \dfrac{i+k}{2} \right\rangle$ is a maximal $\mathbb{Z}$-order in $B_{23,\infty}$, we have $\#\,\mathrm{Cls}_{\mathsf{R}}(O) = 1 + 2 = 3$. Moreover, a maximal $\mathbb{Z}$-order O in a definite quaternion algebra B over $\mathbb{Q}$ has $\#\,\mathrm{Cls}_{\mathsf{R}}(O) = 1$ if and only if $\mathrm{disc}(B) = 2, 3, 5, 7, 13$; i.e. when $\mathrm{disc}(B) = p$ with $g_0(p) = 0$ [Voi21, Theorem 25.4.1, Remark 25.4.2, Remark 41.5.13] [Koh97]. In general, there are exactly 24 isomorphism classes of definite quaternion $\mathbb{Z}$-orders in a definite quaternion algebra over $\mathbb{Q}$ with $\#\,\mathrm{Cls}_{\mathsf{R}}(O) = 1$ [Voi21, Theorem 25.4.3].

Let O be any $\mathbb{Z}$-order in a definite quaternion algebra over $\mathbb{Q}$ with $h := \#\,\mathrm{Cls}_{\mathsf{R}}(O)$. Let $I_1, \ldots, I_h$ be a set of representative[87] invertible right fractional O-ideals for $\mathrm{Cls}_{\mathsf{R}}(O)$ [Voi21, ¶41.2.1]. For $n \in \mathbb{Z}_{\geq 1}$, we define an $h \times h$-matrix $T(n) \in M_h(\mathbb{Z})$ with nonnegative integer entries, called the *n-Brandt matrix*[88], by

$$T(n)_{ij} := \#\{J \subseteq I_j \mid \mathrm{nrd}(J) = n\,\mathrm{nrd}(I_i) \text{ and } [J]_{\mathsf{R}} = [I_i]_{\mathsf{R}}\};$$

i.e. for each j, we consider the set of right invertible O-ideals $J \subseteq I_j$ with $\mathrm{nrd}(J) = n\,\mathrm{nrd}(I_j)$, and we count them according to their class in $\mathrm{Cls}_{\mathsf{R}}(O)$ [Voi21, ¶41.2.2]. If $n = \ell$ is prime and $\ell \nmid \mathrm{discrd}(O)$, then there are exactly $\ell + 1$ such ideals, so the sum of the entries in every column in $T(\ell)$ is equal to $\ell + 1$ [Voi21, pp. 763–764, Proposition 41.3.1]. We define the *Brandt module* $M_2(O)$ to be the $\mathbb{C}$-vector space with basis $\mathrm{Cls}_{\mathsf{R}}(O)$ and equipped with the action of Brandt matrices $T(n)$ for $n \in \mathbb{Z}_{\geq 0}$ on the right [Voi21, p. 765, ¶41.2.5, Exercise 41.1].

```
sage: BM = BrandtModule(23, M=1) #dimension is the class number; their level corresponds to our discrd(O)=pM, M corresponds to our lev(O); modular forms of weight 2 on \Gamma_0(discrd(O))
sage: BM
Brandt module of dimension 3 of level 23 of weight 2 over Rational Field
sage: BM.quaternion_algebra() == B #B_{p,\infty}
True
sage: BM.order_of_level_N() == O #maximal order
True
sage: ClsR = BM.right_ideals() #representative O-ideals for ClsR(O)
sage: ClsR
(Fractional ideal (2 + 2*j, 2*i + 2*k, 4*j, 4*k), Fractional ideal (2 + 2*j, 2*i + 6*k, 8*j, 8*k), Fractional ideal (2 + 10*j + 8*k, 2*i + 8*j + 6*k, 16*j, 16*k))
sage: ClsR[0].is_equivalent(B.ideal(O.basis())) #trivial class
True
sage: ClsR[0].scale(1/4) == B.ideal(O.basis()) #alpha=1/4
True
sage: ClsR[1].is_equivalent(J) #ideal class
True
sage: ClsR[1].scale(1/4) == J #alpha=1/4
True
sage: ClsR[2].is_equivalent(J) #member of only one class
False
sage: MM = BM.hecke_matrix(2) #this is another name for Brandt matrix; here it's actually transpose of the one we defined, hence sum of rows is 2+1=3
```

[87] An algorithm for finding these representatives is given in [KV10, §7].

[88] For an equivalent computationally more efficient definition see [Piz80, Definition 2.13] [Mes86, §2.3] [Déc98, §1.6] [Voi21, ¶41.1.3, Lemma 41.2.7, ¶41.2.11].

```
sage: MM #it is a coincidence that M==MM, in general they are permutations of
    each other
[1 2 0]
[1 1 1]
[0 3 0]
```

1.2.3 Drawing graphs

As above, let O be a $\mathbb{Z}$-order in a definite quaternion algebra over $\mathbb{Q}$. Let $I, J \subseteq O$ be invertible right O-ideals. We say J is a *n-neighbor* of I if $J \subseteq I$ and $n\,\mathrm{nrd}(I) = \mathrm{nrd}(J)$ [Voi21, Definition 41.1.6, Definition 41.2.12]. The *n-Brandt graph* of O is the directed graph with vertices $\mathrm{Cls}_{\mathsf{R}}(O)$ (or $\mathrm{Cls}_{\mathsf{L}}(O)$) and a directed edge from $[I_i]_{\mathsf{R}}$ to $[J]_{\mathsf{R}}$ for each n-neighbor $J \subseteq I_i$. That is, the n-Brandt matrix defined above is simply the adjacency matrix of the n-Brandt graph. In particular, for $n = \ell$ prime and $\ell \nmid \mathrm{discrd}(O)$, we get a $(\ell+1)$-regular (out-degree) directed multigraph and call it *ℓ-Brandt graph*. For example, we can use SageMath to draw 2-Brandt graph when $\mathrm{discrd}(O) = \mathrm{disc}(B) = 23$ [vdLaa18, §7.1] [Voi21, Example 17.6.3, Example 41.1.2, Example 41.1.7]

```
sage: BG = DiGraph(MM, format='adjacency_matrix')
sage: BGG = BG.graphplot(pos=dict(zip(BG, [[-1,0], [1,0], [0,-2]])),
    vertex_labels=dict(zip(BG, ['ClsR[0]', 'ClsR[1]', 'ClsR[2]'])), vertex_size
    =4000, dist=2, loop_size=0.2, edge_thickness=2)
sage: BGG.plot()
Graphics object consisting of 15 graphics primitives
```

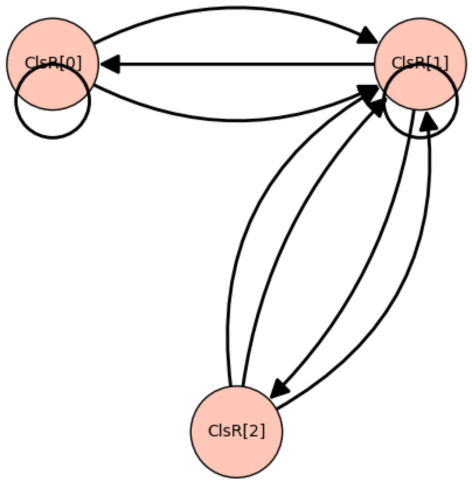


Figure 8: 2-Brandt graph of a maximal order in $B_{23,\infty}$

We can also visualize the ℓ-Brandt graph as the quotient of an *auxiliary graph*. Consider the auxiliary directed graph whose vertices are invertible right O-ideals whose reduced norm is a power of ℓ, and a directed edge exists from I to J if $J \subseteq I$ and $\ell\,\mathrm{nrd}(I) = \mathrm{nrd}(J)$; i.e. J is a ℓ-neighbor of I [Pan21, Proposition 2.65]. The notion of belonging to the same ideal class induces an equivalence relation on this auxiliary graph, and the quotient is the ℓ-Brandt graph [KV10, p. 1740] [Voi21, ¶41.1.9, 41.2.13]. For example, we can use SageMath to check norms of representative ideals in above 2-Brandt graph are powers of 2:

```
sage: ClsR[0].norm()
16
sage: ClsR[1].norm()
32
```

```
sage: ClsR[2].norm()
64
```

Moreover, ℓ-Brandt graphs generally[89] belong to a family of *Ramanujan graphs*[90] [Piz90, §3] [KV10, Theorem 7.6] [Gul20, Day 3 notesand homework]. That is, a $(\ell + 1)$-regular graph on h-vertices such that the absolute value of the second largest eigenvalue of the adjacency matrix, different from $\ell + 1$, is at most $2\sqrt{\ell}$ [LPS88, Definition 1.1]. For example, we can use SageMath to verify this for the above graph:

```
sage: MM.eigenvalues() #3, (-1-sqrt(5))/2, (-1+sqrt(5))/2
[3, -1.618033988749895?, 0.618033988749895?]
sage: bool(abs(MM.eigenvalues()[1]) <= 2*sqrt(2))
True
```

However, it is not difficult to find Ramanujan graphs. Highly nontrivial is the construction of infinite sequences of m-regular Ramanujan undirected[91] graphs on n points, where m is fixed and n tends to infinity [DSV03, Theorem 0.10.10] [BH12, Chapter 4]. For example, the 2-Brandt graphs of maximal order $O \subseteq B_{p,\infty}$ for $p \equiv 1, 121, 169, 289, 361, 529 \pmod{840}$ belong to an infinite sequence of 3-regular (undirected) Ramanujan graphs, starting with $p = 1009$ [Piz98, Example 2]. The families of Ramanujan graphs are one of the best explicit *expander graphs*, i.e. graphs that are simultaneously sparse and highly connected [HLW06, §5.3]. Therefore, combinatorially, Ramanujan graphs are highly connected[92], and hence such graphs can be used in the construction of communication networks [Bie89, §4] [Liv01] [Cha23]. On the other hand, from the probabilistic viewpoint, the natural random walk[93] on Ramanujan graphs converges to its limiting distribution as rapidly as possible, and hence such graphs can be used in cryptography [Cos+19, Part 2].

1.3 Correspondence

To obtain more evidence about the correspondence between supersingular elliptic curves and definite quaternion algebras, one could repeat all the above SageMath computations for $p = 37$ and then check graph isomorphism[94] between 2-isogeny graph and 2-Brandt graph [MS74, §5.1] [Ogg74, Theorem 1] [Piz80, §9] [Mes86, §2.5] [Cer04, Examples 2.2, 3.2, 3.5] [Col22, Appendix B, p. 254] [Arp22, Example 3.7.1]:

```
sage: G.is_isomorphic(BG)
True
```

Elliptic curves are abelian groups, so the K-isogenies between them form groups, denoted by $\mathrm{Hom}_K(E, E')$. Moreover, $\mathrm{Hom}_K(E, E')$ is a torsion-free $\mathbb{Z}$-module of rank at most 4 [Sil09, Proposition III.4.2(b), Corollary III.7.5] [Gal12, Lemma 9.6.11]. If $E = E'$, then we can also compose isogenies, i.e. $\mathrm{Hom}_K(E, E) = \mathrm{End}_K(E)$ is called *endomorphim ring* of E. The invertible elements of $\mathrm{End}(E)$ form the *automorphism group* of E, which is denoted by $\mathrm{Aut}_K(E)$ [Sil09, p. 67] [Gal12, Lemma 9.6.6]. Moreover, $\mathrm{End}_K(E)$ is an associative unital $\mathbb{Z}$-algebra with a standard involution given by the dual $\widehat{\ }$ [Sil09, Theorem III.6.2(b, c, f), §III.9] [Voi21, ¶42.1.3]. Therefore, $\mathrm{End}^0_K(E) \coloneqq \mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an associative $\mathbb{Q}$-algebra called *endomorphism algebra* of E [Hus04, §13.6] [Pan21, §2.4.2] [Sut22, Definition 12.2]. Moreover, $\mathrm{End}^0_K(E)$ is either $\mathbb{Q}$, an imaginary quadratic field, or a definite quaternion algebra over $\mathbb{Q}$ [Sil09, Corollary III.9.4] [Voi21, Lemma 42.1.5] [Sut22, Theorem 12.17]. This was first observed by Helmut Hasse in 1936, and then proved by Max Deuring in 1941 [Deu41]. If $\mathrm{char}(K) = 0$, then $\mathrm{End}^0_K(E)$ is commutative, and hence cannot be a quaternion algebra [Sil09, Corollary III.5.6(c)]. On the other hand, if K is a finite field $\mathbb{F}_q$, then $\mathrm{End}^0_K(E)$ is always larger than $\mathbb{Q}$ [Sil09, Theorem V.3.1(a)(iv), (b)]. That is, the endomorphism algebra has rank 1 or 2 in characteristic 0 but rank 2 or 4 in characteristic $p > 0$ [Hus04, p. 253, 269].

[89] In general, they can be labeled *almost Ramanujan* because the absolute value of the second largest eigenvalue ℓ^r-Brandt undirected graph is at most $(r + 1)\sqrt{\ell^r}$ [Piz90, Theorem 2A] [Piz98, Theorem 5.3] [Ler22, §2.4.3].

[90] The name comes from the fact that the first constructions used the Ramanujan-Petersson Conjecture (proved by Pierre Deligne in 1974) to prove that the graphs constructed had this optimal property (Alon-Boppana bound) [Sar90] [Li96].

[91] That is, in-degree = out-degree. This happens for ℓ-Brandt graphs for maximal orders of $B_{p,\infty}$ when $p \equiv 1 \pmod{12}$ [Piz98, Proposition 4.6].

[92] That is, to disconnect a large part of the graph, one has to sever many edges

[93] That is, we have a token on a vertex, that moves at every step to a random neighboring vertex, chosen uniformly and independently.

[94] This is not an easy thing to do. We will talk about it in §3.2.1.

Deuring coined the term *supersingular*[95] to refer to the elliptic curves[96] with $\mathrm{End}^0_{\overline{K}}(E)$ isomorphic to a definite quaternion algebra over $\mathbb{Q}$ [Roq18, §8.4.1]. Furthermore, he showed the following correspondence between supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and maximal orders of $B_{p,\infty}$ [Deu41, §10.2, p. 265] [Bel08, Theorem 2.2.4] [Roq18, p. 120]:

1. $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ of a supersingular elliptic curve E, is (isomorphic to) a maximal $\mathbb{Z}$-order O in $B_{p,\infty}$ [Déc98, Theorem 2.6(iv)] [Voi21, Theorem 42.1.9].
   - For example, if $E : y^2 = x^3 + x$ over $\mathbb{F}_{23}$, then $\mathrm{End}_{\overline{\mathbb{F}}_{23}}(E) = \mathbb{Z}\left\langle 1, \iota, \frac{\iota + \pi_E}{2}, \frac{1 + \iota\pi_E}{2} \right\rangle$ where $\iota, \pi_E \in \mathrm{End}_{\overline{\mathbb{F}}_{23}}(E)$ such that ι is the map[97] $(x, y) \mapsto (-x, \sqrt{-1}y)$ and π_E is the Frobenius map $(x, y) \mapsto (x^{23}, y^{23})$ [PL17, Prop 2] [Eis+18, Prop 3] [GV18, Example 5] [Ler22, p. 33].
2. Every maximal $\mathbb{Z}$-order O in $B_{p,\infty}$ appears as the endomorphism ring of some elliptic curve E over $\overline{\mathbb{F}}_p$ [Voi21, Corollary 42.2.21].
   - If the unique two-sided integral O-ideal of reduced norm p is principal then there is exactly one supersingular elliptic curve E up to isomorphism over $\overline{\mathbb{F}}_p$, and $j(E) \in \mathbb{F}_p$. On the other hand, if the unique two-sided integral O-ideal of reduced norm p is not principal then there are exactly two supersingular elliptic curves E_1, E_2 up to isomorphism over $\overline{\mathbb{F}}_p$, and $j(E_1), j(E_2) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ are conjugate[98] to each other [Voi21, Lemma 42.4.1]. Therefore, the supersingular ℓ-isogeny graph $G_\ell(p)$ is a 2-covering of the ℓ-ideal graph of $B_{p,\infty}$, except for the vertices defined over $\mathbb{F}_p$ (for which we have a 1-to-1 correspondence) [Amo+21, §2.2.2] [Voi21, Remark 17.4.15]. For example, the 2-ideal graph of $B_{23,\infty}$ is isomorphic to $G_2(23)$ because $23 \in \mathbb{S}$ is one of the supersingular primes.
3. Let E_0 be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_0) \cong O_0 \subseteq B_{p,\infty}$. There is a bijection between isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and the left class set $\mathrm{Cls}_{\mathsf{L}}(O_0)$ [Voi21, Corollary 42.3.7]:

$$\begin{aligned}[E] &\leftrightarrow [I]_{\mathsf{L}}\\ \mathrm{End}_{\overline{\mathbb{F}}_p}(E) &\cong O_{\mathsf{R}}(I)\\ \mathrm{Aut}_{\overline{\mathbb{F}}_p}(E) &\cong O_{\mathsf{R}}(I)^\times\end{aligned}$$

   - The number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ is equal to the class number of maximal orders in $B_{p,\infty}$ [Déc98, Corollary 2.13] [Voi21, ¶42.3.8]. Hence, justifying the relationship between (9) and (20).

In 1969, William Waterhouse introduced the concept of *kernel ideals* to give a more refined formulation of Deuring's correspondence [Wat69, Chapter 3]. Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Let $I \subseteq \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ be a nonzero integral left $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$-ideal. Since $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ is a maximal order of $\mathrm{End}^0_{\overline{\mathbb{F}}_p}(E)$, I is necessarily locally principal (in particular, invertible). Then we can define $E[I] \subseteq E$ to be the scheme-theoretic intersection[99]

$$E[I] := \bigcap_{\phi \in I} \ker(\phi)$$

[95] Before their discovery, curves with endomorphism algebra isomorphic to $\mathbb{Q}$ were called *general* and curves with endomorphism algebra isomorphic to imaginary quadratic fields were called *singular* to mean "quite special." Therefore, Deuring used essentially the same terminology and called the curves with endomorphism algebra isomorphic to definite quaternion algebra to be *supersingular* to mean "more singular than the others." However, in modern terminology we classify elliptic curves as *ordinary* and *supersingular* [Sil09, Remark 3.2.2].

[96] Caution: It is important that we are working with endomorphisms over $\overline{K}$, otherwise we might end up with an imaginary quadratic field as the endomorphism algebra [Sot20, Example 2.13] [Voi21, ¶42.1.6] [Arp22, §1.6.2]. Moreover, as noted earlier, if E is supersingular over charateristic p, then E is isomorphic over $\overline{K}$ to another supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ [Voi21, ¶42.1.8].

[97] To learn more about this map, see [Sil09, Example III.4.4] [Gal12, Example 9.10.20].

[98] That is, if $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ with $\overline{\alpha} = \alpha^p$ then $j(E_1) = u + v\alpha$ and $j(E_2) = u + v\overline{\alpha}$ [Gal12, §6.3].

[99] Here E is a scheme with closed subschemes $\ker(\phi)$ and $\ker(\tau)$ corresponding to quasi-coherent ideal sheaves $\mathcal{A}, \mathcal{B}$. The scheme theoretic intersection of $\ker(\phi)$ and $\ker(\tau)$ is the closed subscheme of E cut out by $\mathcal{A} + \mathcal{B}$: `https://stacks.math.columbia.edu/tag/0C4H`

where $\ker(\phi)$ is a group scheme over $\overline{\mathbb{F}}_p$ [Voi21, ¶42.2.1] [Pan21, Proposition 2.44]. Furthermore, there exists an isogeny $\phi_I : E \to E/E[I]$ with $\deg(\phi_I) = \operatorname{rank}(E[I])$ [Voi21, ¶42.2.3]. On the other hand, given a finite subgroup scheme $H \leq E(\overline{\mathbb{F}}_p)$, we define *kernel ideal*

$$I(H) \coloneqq \{\phi \in \operatorname{End}_{\overline{\mathbb{F}}_p}(E) \mid \phi(P) = 0 \text{ for all } P \in H\} \subseteq \operatorname{End}_{\overline{\mathbb{F}}_p}(E)$$

where $I(H)$ is a left $\operatorname{End}_{\overline{\mathbb{F}}_p}(E)$-ideal. Moreover, $I(H)$ is nonzero because $[\#H] \in I(H)$ [Voi21, ¶42.2.14]. Furthermore, if $\phi : E \to E'$ is an isogeny, then $I_\phi \coloneqq I(\ker(\phi)) \subseteq \operatorname{Brt}(\operatorname{End}_{\overline{\mathbb{F}}_p}(E))$ is an integral $\operatorname{End}_{\overline{\mathbb{F}}_p}(E), \operatorname{End}_{\overline{\mathbb{F}}_p}(E')$-ideal. Therefore, we get the following additional correspondence [Bel08, Proposition 2.2.5] [Voi21, Lemma 42.2.7, Proposition 42.2.16, Corollary 42.2.21, Exercise 42.5 in Addenda] [Arp22, Theorem 1.6.2, Theorem 1.6.5] [Ler22, Proposition 2.1.4, Proposition 2.1.5] [Eri+23, §2.5]:

1. $\deg(\phi_I) = \operatorname{nrd}(I)$ and $\operatorname{nrd}(I_\phi) = \deg(\phi)$
2. $E[I(H)] = H$ and $I(E[I]) = I$ (overloaded notation)
3. $\phi_{\overline{I}} = \widehat{\phi_I}$ (dual isogeny) and $I_{\widehat{\phi}} = \overline{I_\phi}$
4. If $I \sim_{\mathsf{L}} J$ then $E/E[I] \cong E/E[J]$
5. For every isogeny $\phi : E \to E'$, there exists a left $\operatorname{End}_{\overline{\mathbb{F}}_p}(E)$-ideal I and an isomorphism $\rho : E/E[I] \to E'$ such that $\phi = \rho\phi_I$. In particular, if $\phi, \tau : E \to E'$ then $I_\phi \sim_{\mathsf{L}} I_\tau$.
6. If $\phi \in \operatorname{End}_{\overline{\mathbb{F}}_p}(E)$ then I_ϕ is a principal left $\operatorname{End}_{\overline{\mathbb{F}}_p}(E)$-ideal.
7. $\phi_{IJ} = \tau_J \circ \phi_I$ for compatible product IJ with $O_{\mathsf{R}}(I) = O_{\mathsf{L}}(J) = \operatorname{End}_{\overline{\mathbb{F}}_p}(E/E[I])$, $\phi_I \in \operatorname{Hom}_{\overline{\mathbb{F}}_p}(E, E/E[I])$, and $\tau_J \in \operatorname{Hom}_{\overline{\mathbb{F}}_p}(E/E[I], E/[IJ])$; and $I_{\tau\circ\phi} = I_\phi I_\tau$ for $\phi : E \to E'$ and $\tau : E' \to E''$

In 1989, building on the ideas of Jean-François Mestre and Joseph Oesterlé, Kenneth Ribet gave the *base point independent*[100] formulation of Deuring's bijection [Rib89, §3] [Eis+18, §3.1] [LB20, §3A] [Voi21, Corollary 42.4.12] [Pan21, Theorem 2.61] [Col22, Theorem 5.32]:

$$\left\{\begin{matrix}\text{isomorphism classes}\\ \text{of supersingular}\\ \text{elliptic curves over } \overline{\mathbb{F}}_p\end{matrix}\right\} \Big/ \operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \longleftrightarrow \left\{\begin{matrix}\text{maximal } \mathbb{Z}\text{-orders}\\ \text{of } B_{p,\infty}\end{matrix}\right\} \Big/ \operatorname{Typ} \tag{21}$$

In 1996, David Kohel showed that the association from supersingular elliptic curves to quaternion ideals is an equivalence of categories [Koh96, §5.3]. Let $\mathcal{S}$ be the category of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ under isogenies and fix E_0 as a base object. Let $\mathcal{I}$ be the category of left fractional $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_0)$-ideals under homomorphisms of $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_0)$-modules. Then the functor $\operatorname{Hom}(-, E_0)$ from $\mathcal{S}$ to $\mathcal{I}$ is an equivalence of categories [Koh97, Theorem 1] [Ler22, Theorem 2.1.8] [Arp22, §1.6.4] [Eri+23, §2.5]. Furthermore, in its full generality, we can take a category of supersingular elliptic curves with a cyclic M-isogeny and ideals of an Eichler order of level M (i.e. Eichler order has index M in the maximal order). Fix a base point (E_0, C_0), where $C_0 \leq E(\overline{\mathbb{F}}_p)$ is a cyclic subgroup of order M. Then $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_0, C_0)$, the subring of $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_0)$ that maps C_0 to itself, is an Eichler order of level M and reduced discriminant pM in $\operatorname{End}^0_{\overline{\mathbb{F}}_p}(E_0)$. Let $\mathcal{S}_M$ be the category of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ equipped[101] with a cyclic M-isogeny (for some fixed M coprime to p), under isogenies identifying the cyclic subgroups. Let $\mathcal{I}_M$ be the category of left fractional $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_0, C_0)$-ideals, under homomorphisms of $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_0, C_0)$-modules. Then the functor Hom(-$-, (E_0, C_0)$) from $\mathcal{S}_M$ to $\mathcal{I}_M$ is an equivalence of categories [Koh97, §3] [De +20, §4] [Voi21, Remark 42.3.10] [Ler22, §2.3.1]. Therefore, combining (16) and (17), we can count the number of isomorphism classes of supersingular elliptic curves with a cyclic ℓ-isogeny, where ℓ is a prime different from p,

$$\#\mathcal{M}_0(\ell)^{ss}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p) = \frac{(p-1)(\ell+1)}{12} + \epsilon_{p,\ell}$$

[100] As one can observe in the third point of Deuring's correspondence, the bijection is phrased in terms of a *base point*, i.e., a fixed supersingular elliptic curve E_0.

[101] This is also known as *elliptic curves with level structures*, see [Arp22, §3.3] [Col22, §5.2.3] [Bas+23, §3] [CL23, §1.1].

where $\epsilon_{p,\ell}$ is a small value depending on p, ℓ modulo 12 [De +20, §4.3, corrected version]. Therefore, "the Deuring correspondence" is a dictionary between the category of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and the category of quaternion fractional ideals [De +20, Table 1] [Ler22, Table 2.1] [Ver23, Table 2.1].

This correspondence leads to the anticipated connection between supersingular module and Brandt module [Mes86, §2.3] [Gro87, §2] [Rib90, §3] [Déc98, Theorem 2.34] [Koh01, §3] [Bes+21, §5.3] [Voi21, Example 42.3.12] [Cow22, §3.3]. Therefore, the supersingular ℓ-isogeny graphs $G_p(\ell)$ (defined in §1.1.3) also belong to family of Ramanujan graphs[102][JMV05, Appendix A] [CGL08, Theorem 4.2] [CLG09, §4] [Gal12, §25.3.2, 25.3.3] [DJP14, §2.2] [GPS20, §2.3] [Pan21, §2.5.3] [Bas+23, Theorem 3] [CL23, Corollary 1.8]. Moreover, we can use this correspondence to find the set $\mathbb{S}$ of supersingular primes [Mor08]; and show that these primes are the only ones that satisfy a certain conjecture of Erich Hecke relating modular forms of weight 2 to quaternion algebra theta-series [Piz78].

There is also a relative notion of supersingular primes. Given an elliptic curve E defined over $\mathbb{Q}$, a *supersingular prime for E* is a rational prime p such that (i) E has good reduction mod p and (ii) the reduced curve $E_p = E \mod p$ is supersingular then a prime p is said to be *supersingular for E* if the reduction of E modulo p is a supersingular elliptic curve over the residue field $\mathbb{F}_p$. Moreover, in 1987, Noam Elkies showed that every elliptic curve over $\mathbb{Q}$ has infinitely many supersingular primes [Elk87]. However, the set of supersingular primes for any E has asymptotic density zero [Elk91] [Sil09, Theorem V.4.7]. Furthermore, in 2003, David Jao showed that when[103] $g_0(p) = 0$ and E over $\mathbb{Q}$ does not have a supersingular reduction mod p, then there are infintely many supersingular primes for E [Jao03, Theorem 2.1.1]. For example, we can use SageMath to get a list of supersingular primes for $E : y^2 = x^3 + x$ over $\mathbb{Q}$:

```
sage: E.supersingular_primes(40) #p = 3 mod 4; supersingular primes up to 40
[3, 7, 11, 19, 23, 31]
```

Furthermore, the understanding of good reduction also helps us find the supersingular points needed to construct the supersingular module, with the key step being Deuring's reduction theorem [Mes86, §2.4] [Lan87, §13.4, 13.5] [Déc98, §3.2] [Gal99, Theorem 3] [Bel08, §2.3] [Was08, Theorem 10.8] [Brö09, §2] [OS16, §10] [DG16, Proposition 2.5, 2.6] [Roq18, §8.4.4] [CPV20, §5.1] [Col22, Theorem 5.12] [Sut22, Remark 21.12, §21.6]. Here is an illustration of this method using SageMath:

```
sage: #https://github.com/krstnmnlsn/Adventures-in-Supersingularland-Data/blob/
    master/walk.sage
sage: #Given a prime p >= 5, find a supersingular j-invariant; [Bro09]
sage: p = 23
sage: q = next(q for q in Primes() if q%4 == 3 and kronecker_symbol(-q,p) == -1)
sage: q
3
sage: HCP = QuadraticField(-q).hilbert_class_polynomial()
sage: HCP
x
sage: HCP.change_ring(GF(p^2)).any_root() #supersingular j-invariant over F_p^2
0
```

In general, we define[104] the *supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$* to be the directed multigraph $G_\ell(\overline{\mathbb{F}}_p) := G_\ell(p)$ whose vertices belong to the set of $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves $\{E_1, \ldots, E_s\}$ where s is given by (9) and E_i's are representative curves, and there is a directed edge $[E_i, E_{i'}]$ for each equivalence class[105] of ℓ-isogenies from E_i to $E_{i'}$ defined over $\overline{\mathbb{F}}_p$ [Arp22, Definition 1.2.1]. For the purposes of computing isogeny graphs, the vertices are labeled with j-invariants and the isogenies corresponding to edges are stored as kernels, and Vélu's formulas are used to compute the associated isogeny [Koh96, Theorem 80] [Haj23, §4.1]. Thus there are $\ell + 1$ edges with initial vertex E_i corresponding to the $\ell + 1$ cyclic subgroups

[102] We generally have extra restrictions to ensure that the graph is undirected ($j = 0, 1728$ are not supersingular) and, without short cycles [Cos+19, Remark 2.4].

[103] Recall that towards the end of §1.2.2, we saw that such primes correspond to discriminant of quaternion algebras with class number 1.

[104] This is a special case of the more general definition given in [Gal12, §25.3].

[105] Recall that since ℓ is a prime, ℓ-isogenies are cyclic and sperarable. Moreover, two separable isogenies are said to be equivalent if they have the same kernel, i.e. they agree up to post-composition with an automorphism of the codomain curve.

of $E_i[\ell]$, so $G_\ell(\overline{\mathbb{F}}_p)$ is $(\ell+1)$-regular outdegree [Koh96, pp. 87–88]. However, vertices with j-invariant $j = 0$ or 1728 have fewer incoming edges (due to automorphisms) [MT93] [Gal12, Remark 25.3.2] [Sta21]. If we assume that $p \equiv 1 \pmod{12}$, then the graph can be made into an undirected graph by identifying isogenies with their duals [CLG09, §4] [vdLaa18, Remark 3.2.5] [Amo+21, §2.1.2]. Some other important special cases of interest are:

1. the subgraph of $G_\ell(\overline{\mathbb{F}}_p)$ consisting of all vertices whose j-invariants lie in $\mathbb{F}_p$ called the *spine* [Arp+21];

2. the graph $G_\ell(\mathbb{F}_p)$, which has twice the number of vertices in the spine of $G_\ell(\overline{\mathbb{F}}_p)$ [DG16]; and

3. the graph $G_\ell(\mathbb{F}_{p^2})$, which has twice the number of vertices of $G_\ell(\overline{\mathbb{F}}_p)$ and can be partitioned into up to five [106] with vertices corresponding to the trace of Frobenius $t \in \{0, \pm p, \pm 2p\}$ (as in (10)), denoted by $G_\ell(\mathbb{F}_{p^2}, t)$ [AAM19, pp. 273-274].

Moreover, the three graphs corresponding to $t \in \{0, \pm p\}$ are small and each of the graphs corresponding to $t \in \{\pm 2p\}$ is isomorphic to $G_\ell(\overline{\mathbb{F}}_p)$ [AAM19, Theorem 6]. That is, since $E : y^2 = x^3 + x$ over $\mathbb{F}_{23^2}$ has $\mathrm{tr}(\pi_E) = -2 \cdot 23$, for computational purposes we can consider $G_\ell(\overline{\mathbb{F}}_{23})$ to mean the connected component of $G_\ell(\mathbb{F}_{23^2})$ corresponding to the trace of Frobenius -46 [Sot20, §5.1] [Sil21, p. 32]. For example, we can use SageMath to draw $G_2(\mathbb{F}_{23^2}, -46)$ [DG16, Appendix] [Col22, Appendix B]:

```
sage: G0 = E0.change_ring(GF(23^2)).isogeny_ell_graph(2, directed=True,
    label_by_j=True) #edges are 2-isogenies over GF(23^2) between isomorphism
    classes of supersingular elliptic curves with trace of Frobenius -46
sage: GG0 = G0.graphplot(pos=dict(zip(G0, [[0,-2], [1,0], [-1,0]])), vertex_size
    =4000, vertex_labels=True, dist=2, loop_size=0.2, edge_thickness=2)
sage: GG0.plot()
Graphics object consisting of 15 graphics primitives
```

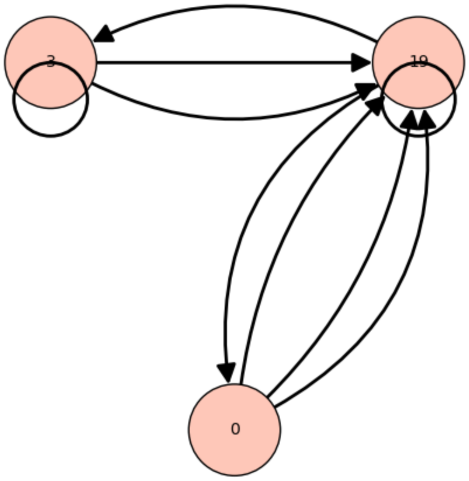


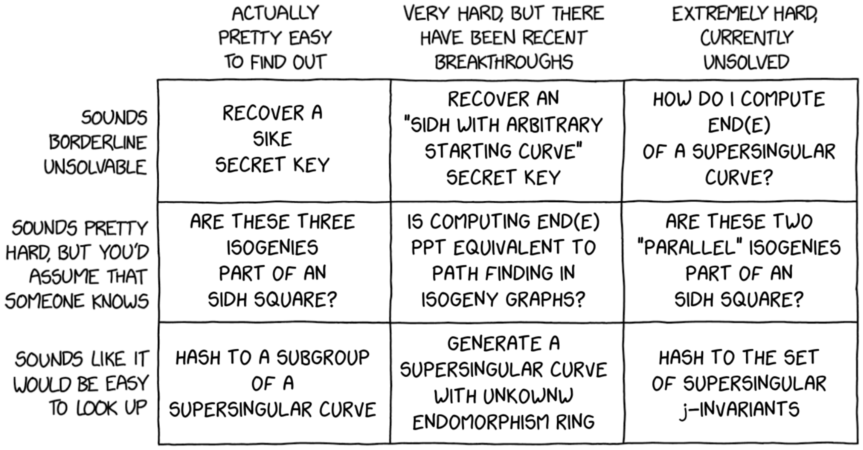
Figure 9: The graph $G_2(\mathbb{F}_{23^2}, -46) \cong G_2(\overline{\mathbb{F}}_{23})$. Morever, since 23 is a supersingular prime, we have $G_2(\overline{\mathbb{F}}_{23})$ equal to its spine.

"I'm so astonished about how happy I am lately: so much time and space for reading, writing, thinking, nicely debating. I truly love my job ;)"
- Sofía Celi (May 30, 2022), https://twitter.com/claucece/status/1531312852597973002

[106] There are two such subgraphs ($t = \pm 2p$) when $p \equiv 1 \pmod{12}$, four subgraphs ($t = \pm p, \pm 2p$) when $p \equiv 5 \pmod{12}$, three subgraphs ($t = 0, \pm 2p$) when $p \equiv -5 \pmod{12}$, and five subgraphs ($t = 0, \pm p, \pm 2p$) when $p \equiv -1 \pmod{12}$.

2 Camera

This section is an *interlude*[107] of this report.



	ACTUALLY PRETTY EASY TO FIND OUT	VERY HARD, BUT THERE HAVE BEEN RECENT BREAKTHROUGHS	EXTREMELY HARD, CURRENTLY UNSOLVED
SOUNDS BORDERLINE UNSOLVABLE	RECOVER A SIKE SECRET KEY	RECOVER AN "SIDH WITH ARBITRARY STARTING CURVE" SECRET KEY	HOW DO I COMPUTE END(E) OF A SUPERSINGULAR CURVE?
SOUNDS PRETTY HARD, BUT YOU'D ASSUME THAT SOMEONE KNOWS	ARE THESE THREE ISOGENIES PART OF AN SIDH SQUARE?	IS COMPUTING END(E) PPT EQUIVALENT TO PATH FINDING IN ISOGENY GRAPHS?	ARE THESE TWO "PARALLEL" ISOGENIES PART OF AN SIDH SQUARE?
SOUNDS LIKE IT WOULD BE EASY TO LOOK UP	HASH TO A SUBGROUP OF A SUPERSINGULAR CURVE	GENERATE A SUPERSINGULAR CURVE WITH UNKOWNW ENDOMORPHISM RING	HASH TO THE SET OF SUPERSINGULAR j-INVARIANTS

Figure 10: *Easy or Hard, isogeny edition!* by Luca De Feo (October 09, 2022) [based on a xkcd comic, with contribution from Andrea Basso, Deirdre Connolly, Tako Boris Fouotsa, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski, `https://twitter.com/luca_defeo/status/1579249496890183680`]

In the previous section, we saw the correspondence that exists between "the world of supersingular elliptic curves over $\overline{\mathbb{F}}_p$" and "the world of quaternion algebra $B_{p,\infty}$." However, in terms of computations, the two worlds are quite different [Koh97, p. 4]. On one hand, in the world of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, it is easy to compute the set of supersingular j-invariants [Bel+09; BLS12; Haj23], but computing the endomorphism ring [EHM17; Ban+19; LOX20; Eis+20; Fus+23] and isogeny between two elliptic curves [Gal99; Shu09; GS13; DG16; Ber+20; LB20; Ben+23] are believed to be difficult. On the other hand, in the world of quaternion algebra $B_{p,\infty}$, determining the ideal class set is difficult [KV10, Theorem B], but its easy to find maximal orders [Ibu82; Voi13] and connecting ideals [KV10, §3] [Koh+14; PS18].

Furthermore, as stated in (21), there exists a one-to-one correspondence between supersingular j-invariants and maximal orders in a quaternion algebra, up to some equivalence relations [Cer04; LM04]. That is, theoretically, it is possible to translate the hard problem from one "world" to the corresponding easy problem in the other. However, finding a maximal quaternion order such that it is isomorphic to the endomorphism ring of a given elliptic curve is believed to be quite difficult [McM14]. On the contrary, it is easy to find a supersingular j-invariant such that the endomorphism ring of $E(j)$ is isomorphic to a given maximal quaternion order [CG14; PL17; Eri+23]. Moreover, this correspondence also gives us an efficient method for computing modular forms [Mes86; Déc98; Cow22].

In fact, the problems of computing an isogeny between supersingular elliptic curves, the endomorphism ring of an elliptic curve, and a maximal quaternion order isomorphic to a given endomorphism ring are all known to be equivalent [Eis+18; Wes22; PW23; Arp+23; MW23].

The reputation of supersingular elliptic curves in cryptology has been dynamic[108] [Gal01]. Likewise, Deuring correspondence can be seen as a double edged sword in cryptology[109]. In the next section we will look at its constructive aspect.

```
"However, I should also mention another option that not very many people consider:
Instead of delving into some other existing field that has depth, try inventing new
applications of the math that you already know.  I did it.  This is really hard, but
really rewarding, because the applications you invent are guaranteed to be tailored
towards your interests!"
- David Jao (September 24, 2020), https://www.reddit.com/r/math/comments/iwx5zb/comment/g6eez2d
```

[107] In a music album, an interlude serves as a connection between two songs. Though the songs can stand on their own, artists include interludes to show the songs are thematically related. Thus the interludes can help show the relationship between two ideas and present them as a greater whole. For example, checkout the album KARAM by KSHMR.

[108] The SIDH fiasco: `https://www.esat.kuleuven.be/cosic/blog/an-efficient-key-recovery-attack-on-sidh/`

[109] A knowledge base of most isogeny based cryptosystems and the best attacks on them: `https://issikebrokenyet.github.io/`

3 Action

3.1 Zero-knowledge proofs

3.1.1 Σ-protocols

Σ-protocol as an abstract concept was introduced by Ronald Cramer in 1997, where the first part of *Sigma* refers to "zig-zag" symbolizing the three-moves, while the last part is an abbreviation of "Merlin-Arthur"[110] [Cra97, p. 19].

In 1990, Claus Schnorr published[111] an *identification protocol.* That is, a protocol involving two parties, a *prover* P and a *verifier* V, such that P has a *secret key* that it uses to convince V of its identity and V has a corresponding *verification key* that it uses to confirm P's claim [BS23, §18.2]. Let p be a prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ has order $\varphi(p) = p - 1$, and $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be an element of order ℓ, where ℓ is a prime divisor of $p-1$. P randomly chooses (secret key) $x \in \mathbb{Z}/\ell\mathbb{Z}$ and publishes (public key) $h \coloneqq g^x \pmod{p}$. V knows that p, ℓ, g, h are such that p, ℓ are prime, and $\mathrm{ord}(g) = \mathrm{ord}(h) = \ell$; i.e. $h \in \langle g \rangle$ and $h = g^x$ for some $0 \leq x \leq \ell - 1$. But V doesn't know whether P knows such a x. The following protocol lets P prove "knowledge" of a discrete logarithm x to V, and was the first efficient Σ-protocol [Dam10, §1]:

1. P randomly chooses $y \in \mathbb{Z}/\ell\mathbb{Z}$ and sends $a \coloneqq g^y \pmod{p}$ as *commitment* to V.

2. V chooses a *challenge* r at random in $\mathbb{Z}/2^t\mathbb{Z}$ (challenge space) and sends it to P. Here t is fixed such that $2^t < \ell$.

3. P sends $z \coloneqq y + rx \pmod{\ell}$ as *response* to V, who checks that $g^z \overset{?}{=} ah^r \pmod{p}$.

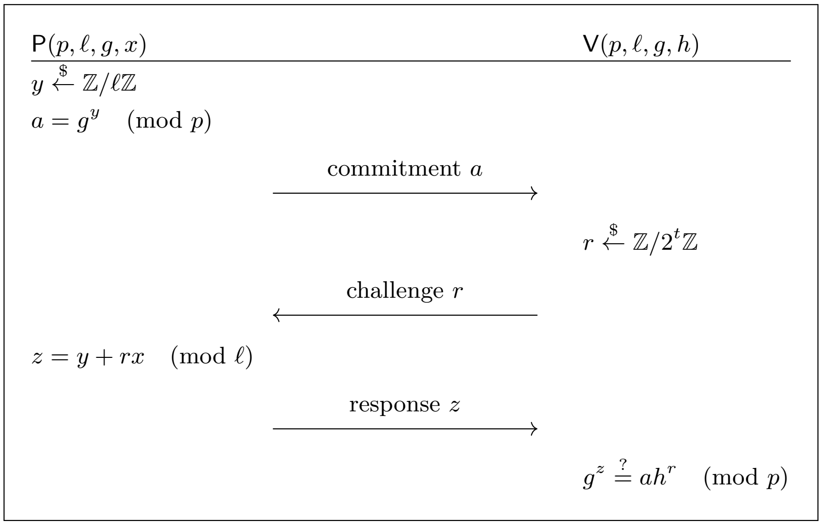

$\mathsf{P}(p, \ell, g, x)$
$\mathsf{V}(p, \ell, g, h)$
$y \overset{\$}{\leftarrow} \mathbb{Z}/\ell\mathbb{Z}$
$a = g^y \pmod{p}$
commitment a
$r \overset{\$}{\leftarrow} \mathbb{Z}/2^t\mathbb{Z}$
challenge r
$z = y + rx \pmod{\ell}$
response z
$g^z \overset{?}{=} ah^r \pmod{p}$

Figure 11: Schnorr identification protocol

This protocol is a *proof of knowledge* because for any h and any pair of accepting conversations, (a, r, z), (a, r', z') where $r \neq r'$, one can efficiently compute $x = (z - z')(r - r')^{-1} \pmod{\ell}$ such that $h = g^x \pmod{p}$. Moreover, the error probability for this proof is $1/2^t$. On the other hand, this protocol is NOT known to be *zero-knowledge*[112] because in order for the problem of finding x to be non-trivial, ℓ must be (exponentially) large, and to achieve negligible error in a single run of the protocol, 2^t must be exponentially

[110] **MA** is the class of problems solvable by Merlin-Arthur games, which involve two players named Merlin (magician) and Arthur (king). For its definition, see `https://complexityzoo.net/Complexity_Zoo:M#ma`

[111] `U.S. Patent 4,995,082`, filed February 23, 1990, granted February 19, 1991, and expired February 23, 2010.

[112] It comes in three flavors: (1) *perfect zero-knowledge* if simulation is identical to true protocol runs; (2) *statistical zero-knowledge* if simulation and true protocol runs have small statistical distance; and (3) *computational zero-knowledge* if simulation and true protocol runs are only indistinguishable by a computationally bounded adversary [Sma16, pp. 427–428] [Sil21, p. 6] [Beu+23, pp. 3435–3436].

large too. However, this protocol is *honest verifier zero-knowledge* because for randomly chosen $z \in \mathbb{Z}/\ell\mathbb{Z}$ and $r \in \mathbb{Z}/2^t\mathbb{Z}$, with $a \coloneqq g^z h^{-r} \pmod{p}$, the conversation (a, r, z) has the same probability distribution as real conversations between the honest prover and the honest verifier. Note that since g^z is uniform in $\langle g \rangle$ and r is also uniform, we get that $a = g^z h^{-r}$ is also uniform. Moreover, z is a deterministic function of a and r [Ven15, Lemma 3].

In the next few paragraphs, we will define some abstract properties which capture the essence of the Schnorr protocol [Dam10] [Ven15] [Tha22, §12.2.1].

Let $\mathcal{R} \subseteq \{0,1\}^* \times \{0,1\}^*$ be a binary relation that defines a **NP** complexity class language $L_{\mathcal{R}} \coloneqq \{y \in \{0,1\}^* \mid (x, y) \in \mathcal{R} \text{ for some } x \in \{0,1\}^*\}$. That is, a string $v \in L_{\mathcal{R}}$ iff there exists a w and polynomial $f : \mathbb{N} \to \mathbb{N}$ such that $|w| \leq f(|v|)$ and $(v, w) \in \mathcal{R}$. Here $|\cdot|$ denotes the length of string. Moreover, such a w is called a *witness* for membership of $v \in L_{\mathcal{R}}$ [Gol01, Definition 1.3.2] [Sma16, §21.3.2] [BS23, Definition 20.1]. For example, for the Schnorr protocol we have discrete logarithm relation given by

$$\mathcal{R} = \mathcal{DL} \coloneqq \{(v, w) \mid v = (p, \ell, g, h), w = x\}$$

where it is understood that p and ℓ are primes with $g, h \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $\operatorname{ord}(g) = \operatorname{ord}(h) = \ell$, and $h = g^x$ for some $x \in \mathbb{Z}/\ell\mathbb{Z}$.

Both, the prover P and the verifier V, are modeled by *probabilistic polynomial time* Turing machines. That is, a probabilistic machine that independently of the outcome of its internal coin tosses halts after a polynomial (in the length of the input) number of steps [Gol01, §1.3.2.2]. Therefore, P's only advantage over V is the knowledge of witness w. For example, the Schnorr protocol implicitly assumes this behavior.

Moreover, if v is the common input to P, V and w be a private input to P such that $(v, w) \in \mathcal{R}$, then we consider the following class of *three-move interactive protocols* for $\mathcal{R}$:

1. P sends a random *commitment* message a.

2. V sends a random *challenge* t-bit string r.

3. P sends a *response* z, and V decides to accept or reject based on the available data v, a, r, z.

This three-move interactive protocol is said to have *completeness* property if V always accepts when there exists a witness w for the common input v. For example, the Schnorr protocol satisfies completeness because

$$g^z \equiv g^{y+rx} \equiv g^y \cdot (g^x)^r = ah^r \pmod{p}$$

Therefore, such a protocol also satisfies the basic *correctness requirement* that any identification protocol must satisfy.

Furthermore, such a three-move interactive protocol is said to have *special soundness* property if from any v, and any pair of accepting conversations on input v, $(a, r, z), (a, r', z')$ where $r \neq r'$ one can efficiently computer w such that $(v, w) \in R$. The special soundness property implies that this three-move interactive protocol is always an interactive proof system for $L_{\mathcal{R}}$ with error probability 2^{-t}. For example, the Schnorr protocol satisfies special soundness as explained above while discussing "proof of knowledge." That is, this protocol is a proof system for $L_{\mathcal{DL}}$. Moreover, this protocol is secure against *direct attacks* [BS23, Theorem 19.1]. We can also show that such an interactive protocol also satisfies *knowledge soundness* for a large challenge space [Ven15, Theorem 1] [Dam10, Theorem 1] [BS23, Definition 19.4].

The above three-move interactive protocol described is said to have *special honest verifier zero-knowledge* property if there exists a polynomial time algorithm, called an *efficient simulator* S, that on taking common input v and challenge r, but without access to the witness w, generates accepting conversation (a, r, z), with the same probability distribution as conversations between the honest prover and the honest verifier on input v. For example, the Schnorr protocol satisfies the honest verifier zero-knowledge property because, as discussed above, the simulator S takes input $v = (p, \ell, g, h)$, and then randomly samples $r \in \mathbb{Z}/2^t\mathbb{Z}$ and $z \in \mathbb{Z}/\ell\mathbb{Z}$, and computes $a \coloneqq g^z h^{-r} \pmod{p}$ to generate accepting conversation with the same probability distribution as real conversations between the honest prover and the honest verifier. This implies the special honest verifier zero-knowledge property. Therefore, this protocol is secure against *eavesdropping attacks* [Gal12, Theorem 22.1.5] [BS23, Theorem 19.3].

We are now ready to state the formal definition. A Σ-*protocol* (P,V) for a relation $\mathcal{R}$ is a three-move interactive protocol with conversation transcripts (a,r,z), where the prover P speaks first, satisfying the three properties[113] (1) completeness; (2) special soundness; and (3) special honest verifier zero-knowledge.

Furthermore, we note the two important facts about Σ-protocols [Dam10, §2]: (1) the properties of Σ-protocols are invariant under parallel composition, i.e. repeating a Σ-protocol for $\mathcal{R}$ (with challenges of length t-bits) twice in parallel produces a new Σ-protocol for $\mathcal{R}$ (with challenges of length $2t$-bits); and (2) if a Σ-protocol for relation $\mathcal{R}$ exists, then for any $t > 0$, there exists a Σ-protocol for $\mathcal{R}$ with challenges of length t-bits. Finally, a Σ-protocol (P,V) for a relation $\mathcal{R}$ with a key generation algorithm G gives an identification scheme secure against eavesdropping attacks [Sma16, §21.3.3] [BS23, Theorem 19.14].

3.1.2 Fiat-Shamir transformation

In 1986, Amos Fiat and Adi Shamir came up with the idea of using a cryptographic hash function in place of the verifier to do non-interactive proofs. Later, in 1993, this was formalized as the random oracle model by Mihir Bellare and Phillip Rogaway [Dam10, §12]. Finally, in 2000, David Pointcheval and Jacques Stern showed that applying the Fiat-Shamir transformation to any Σ-protocol (such as Schnorr's) yields a non-interactive argument of knowledge in the random oracle model [Tha22, §12.2.3].

Consider the same setup as for the Schnorr identification protocol discussed above. Let p be a prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ has order $\varphi(p) = p-1$. Let ℓ be a prime divisor of $p-1$ and $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be an element of order ℓ. The *key generation algorithm* G randomly chooses *private key* $x \in \mathbb{Z}/\ell\mathbb{Z}$ and public key $h = g^x \pmod{p}$. The public information includes p, ℓ, g, h such that p, ℓ are known to be prime, and $\operatorname{ord}(g) = \operatorname{ord}(h) = \ell$. That is, $h \in \langle g \rangle$ and $h = g^x$ for some $0 \le x \le \ell - 1$. Using a cryptographic hash function $\mathsf{H} : \mathfrak{M} \times \langle g \rangle \to \mathbb{Z}/2^t\mathbb{Z}$, where t is fixed such that $2^t < \ell$ for challenge space $\mathbb{Z}/2^t\mathbb{Z}$ and $\mathfrak{M}$ is the message space, we can transform the Schnorr identification protocol into the following signature scheme [BS23, §19.2]:

1. To sign a message $m \in \mathfrak{M}$ using secret key x, the *signing algorithm* randomly chooses $y \in \mathbb{Z}/\ell\mathbb{Z}$ and computes $a = g^y \pmod{p}$. Then it computes $r = \mathsf{H}(m,a)$ and $z = y + rx \pmod{\ell}$ to produce the signature $\sigma \coloneqq (a,z)$.

2. To verify the signature $\sigma = (a,z)$ on a message m using the public key h, the signature *verification algorithm* computes $r = \mathsf{H}(m,a)$ and checks that $g^z \overset{?}{=} ah^r \pmod{p}$.

```
Signing $(p, \ell, g, h, m, \mathsf{H}, x)$
$y \xleftarrow{\$} \mathbb{Z}/\ell\mathbb{Z}$
$a = g^y \pmod{p}$
$r = \mathsf{H}(m,a)$
$z = y + rx \pmod{\ell}$
return $\sigma \coloneqq (a,z)$
```

```
Verification $(p, \ell, g, h, m, \mathsf{H}, \sigma)$
$r = \mathsf{H}(m,a)$
return $g^z \overset{?}{=} ah^r \pmod{p}$
```

Figure 12: Schnorr signature scheme

The Fiat-Shamir transformation exploits the fact that the Σ-protocol is public coin, so the challenges sent by the verifier are uniformly random, and thus can be replaced by a hash of the statement and the previous messages without affecting the distribution of the transcripts [Sil21, Theorem 1]. Moreover, if we model H as a random oracle[114], then Schnorr signature scheme is secure[115] because Schnorr identification

[113] Some authors do not include these three properties in the definition of Σ-protocol. For example, in [GPS20, p. 142] and [Ler22, §5.1.1], a Σ-protocol is defined as a 3-round public-coin interactive protocol between a prover and a verifier. Here, *public-coin* means that the messages are uniformly random and independent from each other [Sil21, §2.2.4].

[114] This is an entity that initially chooses (in private) a random function $\mathsf{H} : \{0,1\}^s \to \{0,1\}^t$ for some s,t. Then any player can send any bit string $m\|a$ of length s to the oracle which will then return $\mathsf{H}(m\|a)$. Since H was completely random, $\mathsf{H}(m\|a)$ is a uniformly chosen string of length t, and is independent of $m\|a$ [Dam10, §10].

[115] That is, unforgeable under chosen message attacks.

protocol is secure against eavesdropping attacks [Gal12, §22.1.3] [BS23, Theorem 19.7]. However, there exist protocols that are secure in the random oracle model but can never be secure for any possible instantiation of the cryptographic hash function [Ven15, §4.3].

We are now ready to state the formal definition. Consider a Σ-protocol (P, V) for a relation $\mathcal{R}$ with conversation of the form (a, r, z), where $a \in \mathfrak{A}$ (commitment space), $r \in \mathfrak{C}$ (challenge space) and $z \in \mathfrak{R}$ (response space). Moreover, let G be the key generation algorithm for $\mathcal{R}$ and $\mathsf{H} : \mathfrak{M} \times \mathfrak{A} \to \mathfrak{C}$ be a cryptographic hash function modeled as a random oracle. Then the *Fiat-Shamir signature scheme* derived from G and (P, V) works as follows [BS23, §19.6.1]:

1. G creates a public key $v \in \{0,1\}^*$ and a secret key $(v, w) \in \mathcal{R}$.
2. To sign a message $m \in \mathfrak{M}$ using secret key (v, w), the signing algorithm runs as follows:
   (a) starts the prover $\mathsf{P}(v, w)$, obtaining a commitment $a \in \mathfrak{A}$.
   (b) computes a challenge $r = \mathsf{H}(m, a) \in \mathfrak{R}$.
   (c) feeds r to the prover P obtaining a response $z \in \mathfrak{R}$, and outputs the signature $\sigma \coloneqq (a, z) \in \mathfrak{A} \times \mathfrak{R}$.
3. To verify a signature $\sigma = (a, z) \in \mathfrak{A} \times \mathfrak{R}$ on a message $m \in \mathfrak{M}$ using a public key v, the verification algorithm computes $r = \mathsf{H}(m, a)$ and checks that $\mathsf{V}(a, r, z)$ is an accepting conversation for v.

As in the case of Schnorr, Fiat-Shamir signature scheme for any Σ-protocol is secure in the random oracle model [Sma16, §21.3.4] [BS23, Theorem 19.16]. However, the security of the Fiat–Shamir transform against quantum adversaries is a topic of ongoing research. In the context of post-quantum cryptography, the Unruh transform offers an alternative, albeit less efficient construction [Sil21, Theorem 3].

3.2 Signature schemes

3.2.1 GPS (Galbraith-Petit-Silva)

This was one of two signature schemes introduced by Steven Galbraith, Christophe Petit, and Javier Silva in 2017 [GPS20, §4]. The GPS identification protocol is based on a Σ-protocol very similar to the zero-knowledge proof of graph isomorphism[116], in which we reveal one of two graph isomorphisms, but never enough information to deduce the secret isomorphism [Sma16, §21.1] [Beu+23, §3.3]. Moreover, just like the protocol for graph isomorphisms, GPS is not very practical because the data structures required are very large, and the protocol needs to be repeated a large number of times before the verifier is convinced that prover really knows the secret [Sma16, p. 429]. One obtains a signature scheme by applying the Fiat-Shamir transformation.

Let p, ℓ be two different primes, fix[117] a supersingular elliptic curve E_0 in characteristic p, and let $j_0 \coloneqq j(E_0)$ be a supersingular invariant in characteristic p. We define a *random isogeny step* of degree ℓ from j_0 as the process of randomly and uniformly choosing a neighbor of j_0 in $G_\ell(p)$, and returning that vertex. For a composite degree $\ell_1\ell_2$, where ℓ_1, ℓ_2 are primes different from p but need not be distinct, we define a *random isogeny walk* of degree $\ell_1\ell_2$ from j_0 as a sequence of j-invariants $\{j_1, j_2\}$ such that j_i is a random step of degree ℓ_i from j_{i-1}. Here we will be using random walks of $\mathcal{B}$-powersmooth degree L, namely $L = \prod_{i=1}^{n} \ell_i^{e_i}$, with all prime powers $\ell_i^{e_i} \leq \mathcal{B} \leq \ell_i^{e_i+1}$, with $\mathcal{B}$ as small as possible and $\gcd(L, p) = 1$, i.e. $\ell_1, \ell_2, \ldots, \ell_n$ be prime numbers different from p [GPS20, §2.3] [Sil21, §5.1].

Let λ be the security parameter, p be a prime with 2λ bits, t be fixed such that $t = \lambda$ or $t = 2\lambda$, $L \coloneqq \prod_{i=1}^{n} \ell_i^{e_i}$, $L' \coloneqq \prod_{i=1}^{n'} \ell_i'^{e_i'}$ be $\mathcal{B}$-powersmooth numbers that are product of prime powers up to $\mathcal{B} \approx 2(1+\varepsilon)\log(p)$ such that $\gcd(L, L') = 1$ [GPS20, Lemma 1] [Sil21, Lemma 21]. The prover P takes a random isogeny walk (secret key) $\phi : E_0 \to E_1$ of degree L and publishes (public key) E_1. The verifier V knows p, $\mathcal{B}$, L, L', E_0, $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_0)$, and E_1. However, V doesn't know whether P knows $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_1)$, or equivalently, a path $\phi : E_0 \to E_1$. Therefore, P can use the following Σ-protocol to prove knowledge of $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_1)$ [Sil21, Theorem 26]:

[116] This problem is believed to lie between the complexity classes **P** and **NP**-complete, i.e. it can neither be solved in polynomial time, nor is it **NP**-complete. However, this problem lies in complexity class **CZK** of all decision problems whose solutions can be verified using a computational zero-knowledge proof [Sma16, §21.2].

[117] For the isogeny-based protocols discussed in this report, we will fix $E_0 : y^2 = x^3 + x$ because we know its endomorphim ring. This is also an example of *special extremal curve* [Koh+14, §2.3] [Ler22, Remark 3.1.2].

1. P takes t random isogeny walks starting from E_1 of $\mathcal{B}$-powersmooth degree L', obtaining curves $E'_1, E'_2, \dots, E'_t$ and isogeny paths $\phi_i : E_1 \to E'_i$.

$$\begin{tikzcd}
 & E_0 \arrow[r, "\phi"] & E_1 \arrow[dll, "\phi_1"'] \arrow[dl, "\phi_2"] \arrow[d] \arrow[dr] \arrow[drr, "\phi_t"] & & \\
E'_1 & E'_2 \arrow[rrr, dash, dotted] & {} & {} & E'_t
\end{tikzcd}$$

   P sends $(E'_1, E'_2, \dots, E'_t)$ as commitment to V.

2. V sends random challenge bit string $b = (b_1, \dots, b_t) \in \{0,1\}^t$ to P (big enough challenge space).

3. P sends response $(\eta_1, \eta_2, \dots, \eta_t)$ to V, with

$$\eta_i \coloneqq \begin{cases} \phi_i : E_1 \to E'_i & \text{if } b_i = 0; \\ \tau_i : E_0 \to E'_i & \text{if } b_i = 1 \end{cases}$$

   where τ_i is computed[118] as follows:

   (a) *Isogeny to O_0O'-ideal:* The L_1-isogeny $\phi : E_0 \to E_1$ was computed as the chain of isogenies $\mu_i : \widetilde{E}_{i-1} \to \widetilde{E}_i$ of degree $\ell_i^{e_i}$, where $i = 1, 2, \dots, n$ with $\widetilde{E}_0 = E_0$ and $\widetilde{E}_n = E_1$:

$$E_0 \xrightarrow{\mu_1} \widetilde{E}_1 \xrightarrow{\mu_2} \cdots \xrightarrow{\mu_n} E_1$$

   Then, as discussed[119] in §1.3, let $I_0 = O_0 = \mathrm{End}_{\overline{\mathbb{F}}_p}(E_0)$, and $I_i \coloneqq \ker(\mu_i \circ \mu_{i-1} \circ \cdots \circ \mu_1)$ be the kernel ideal of the isogeny $E_0 \to \widetilde{E}_i$. We then have

$$I_i = I_{i-1}\ell_i^{e_i} + I_{i-1}\alpha$$

   where $\alpha \in I_0$ such that $\ker(\phi) \cap E_0[\ell_i^{e_i} O_0] \subseteq \ker(\alpha)$ and $\gcd\left(\deg(\alpha), \ell_i^{e_i+1}\right) = \ell_i^{e_i}$ [GPS20, p. 134] [Sil21, Proposition 5, Equation 2.5] [Voi21, Exercise 10.7]. Hence, P computes an element $\alpha_i \in I_{i-1}$ and an ideal $I_i = I_{i-1}\ell_i^{e_i} + O_0\alpha_i$ for $i = 1, \dots, n$. Then $I = \prod_{i=1}^{n} I_i$ is the left O_0-ideal corresponding to the secret isogeny $\phi : E_0 \to E_1$, i.e. $O_{\mathsf{R}}(I) = O_1 \coloneqq \mathrm{End}_{\overline{\mathbb{F}}_p}(E_1)$. Similarly, P computes the left O_1-ideal I' corresponding to L'-isogeny $\phi_i : E_1 \to E'_i$ with $O_{\mathsf{R}}(I') = O' \coloneqq \mathrm{End}_{\overline{\mathbb{F}}_p}(E'_i)$. Finally, P computes the ideal product II', to obtain the O_0O'-ideal corresponding to $\phi_i \circ \phi$.

   (b) *O_0O'-ideal of norm L':* Starting with maximal order O_0 and left O_0-ideal II', P solves the *quaternion L'-isogeny problem* to get an equivalent[120] left O_0-ideal J of reduced norm L' with $O_{\mathsf{R}}(J') = E'_i$ [Ray18, §3.2] [GPS20, §4.3].

   (c) *O_0O'-ideal to isogeny:* Given E_0, O_0, E'_i, J such that $O_{\mathsf{L}}(J) = O_0$ and $O_{\mathsf{R}}(J) = O'$, P computes[121] a sequence of prime degree isogenies giving the isogeny $\tau_i : E_0 \to E'_i$.

   Then V checks if each η_i is the correct isogeny path.

The GPS Σ-protocol achieves statistical zero-knowledge [Beu+23, Remark 3]. While polynomial time in theory, the resulting signature scheme is considered impractical.

[118] We need an isogeny that does not leak any information about ϕ. That is, $\tau_i \neq \phi_i \circ \phi$.

[119] Also recall that for any M-isogeny $\phi : E_0 \to E_1$ of we can associate a left O_0-ideal $I = \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_1, E_0)\phi$ of norm M.

[120] Note that the ideals returned by the quaternion L'-isogeny algorithm correspond to vertices of the path in the L'-Brandt graph, and to a sequence of j-invariants by Deuring's correspondence [GPS20, p. 160].

[121] This step is a rather more theoretical than practical algorithm, particularly when required to translate ideals with large norm L'. Therefore, GPS was never implemented [Ler22, p. 123].

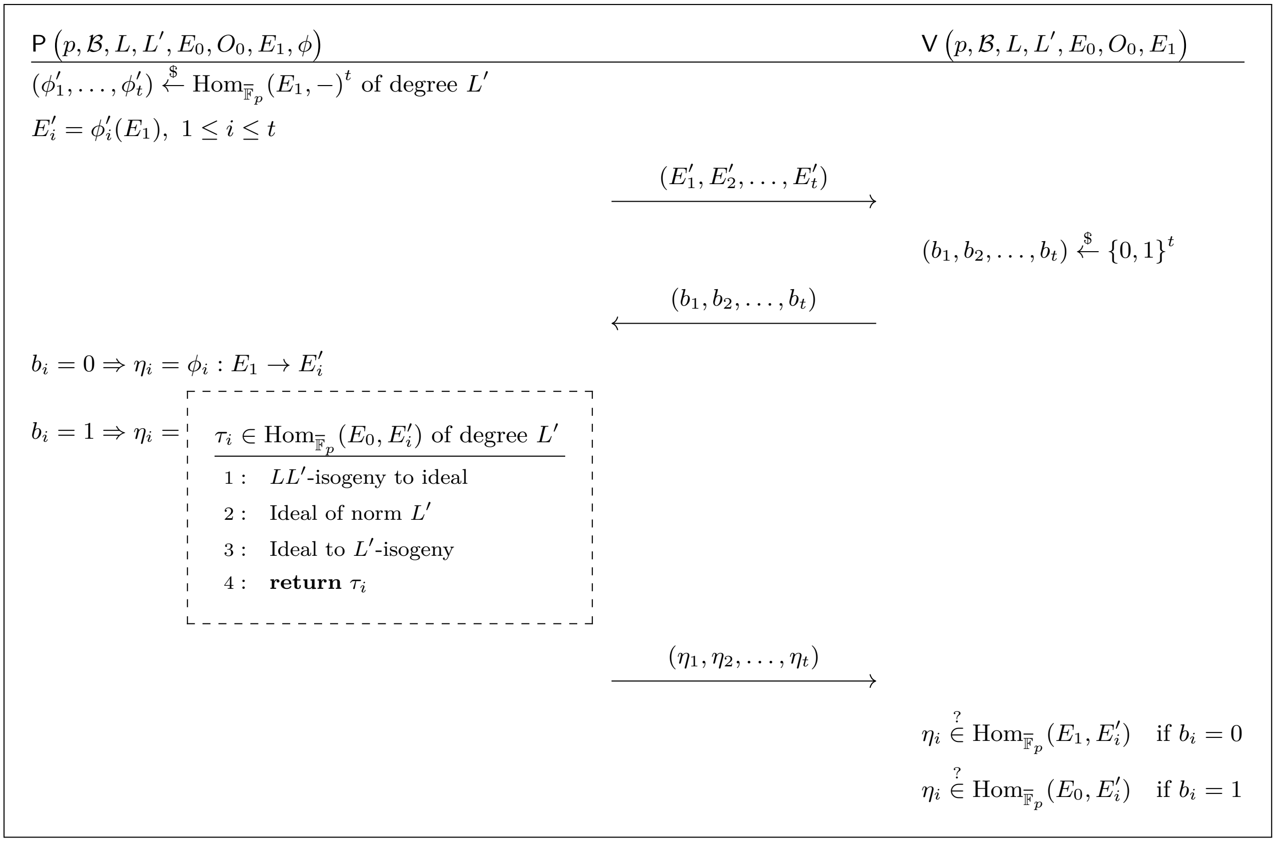

$\mathsf{P}\left(p, \mathcal{B}, L, L', E_0, O_0, E_1, \phi\right)$
$\mathsf{V}\left(p, \mathcal{B}, L, L', E_0, O_0, E_1\right)$
$(\phi'_1, \ldots, \phi'_t) \overset{\$}{\leftarrow} \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_1, -)^t$ of degree L'
$E'_i = \phi'_i(E_1),\ 1 \le i \le t$
$(E'_1, E'_2, \ldots, E'_t)$
$(b_1, b_2, \ldots, b_t) \overset{\$}{\leftarrow} \{0,1\}^t$
$(b_1, b_2, \ldots, b_t)$
$b_i = 0 \Rightarrow \eta_i = \phi_i : E_1 \to E'_i$
$b_i = 1 \Rightarrow \eta_i =$
$\tau_i \in \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_0, E'_i)$ of degree L'
1 : LL'-isogeny to ideal
2 : Ideal of norm L'
3 : Ideal to L'-isogeny
4 : **return** τ_i
$(\eta_1, \eta_2, \ldots, \eta_t)$
$\eta_i \overset{?}{\in} \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_1, E'_i)$ if $b_i = 0$
$\eta_i \overset{?}{\in} \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_0, E'_i)$ if $b_i = 1$

Figure 13: GPS identification protocol

Consider the same setup as for the GPS identification protocol discussed above. Given the security parameter λ, the key generation algorithm G randomly chooses a prime $p \equiv 3 \pmod 4$ with 2λ bits, fixes t such that $t = \lambda$ or $t = 2\lambda$, $L := \prod_{i=1}^{n} \ell_i^{e_i}$, $L' := \prod_{i=1}^{n'} \ell_i'^{e'_i}$ are $\mathcal{B}$-powersmooth numbers that are product of prime powers up to $\mathcal{B} \approx 2(1+\varepsilon)\log(p)$ such that $\gcd(L, L') = 1$. It performs a random isogeny walk of degree L from the curve E_0 with j-invariant $j_0 = 1728$ to a curve E_1 with j-invariant j_1. Then it computes the left O_0-ideal I corresponding to this isogeny with $O_{\mathsf{R}}(I) = O_1 := End_{\overline{\mathbb{F}}_p}(E_1)$. Choose a cryptographic hash function $\mathsf{H} : \mathfrak{M} \times \mathfrak{A} \to \{0,1\}^t$, where $\mathfrak{A}$ is the set of j-invariant tuples of size t representing supersingular elliptic curves in characteristic p, and $\mathfrak{M}$ is the message space. The public key is (p, j_1, H) and the secret key is O_1, or equivalently I. We can use Fiat-Shamir heuristic to transform the GPS identification protocol into the following signature scheme [GPS20, §4.5] [Sil21, §5.3.5]:

1. To sign a message $m \in \mathfrak{M}$ using secret key O_1, the signing algorithm generates random isogeny walks $\phi'_1, \phi'_2 \ldots, \phi'_t$, starting from j_1, of B-powersmooth degree L', ending at j-invariants $j'_1, j'_2, \ldots, j'_t$, respectively. Then it computes $b = (b_1, \ldots, b_t) := \mathsf{H}(m, j'_1, \ldots, j'_t)$ and $\eta = (\eta_1, \ldots, \eta_t)$ such that
$$\eta_i = \begin{cases} \psi_i : L'\text{-isogeny path from } j_1 \text{ to } j'_i & \text{if } b_i = 0 \\ \tau_i : L'\text{-isogeny path from } j_0 \text{ to } j'_i & \text{if } b_i = 1 \end{cases}$$
to produce the signature $\sigma := (b, \eta)$.

2. To verify the signature $\sigma = (b, \eta)$ on a message m using the public key j_1, the signature verification algorithm uses the paths η_i to recover the j-invariants j'_i, for $1 \le i \le t$, and checks that $b \overset{?}{=} \mathsf{H}(m, j'_1, \ldots, j'_t)$.

This signature scheme served as a motivation behind the signature scheme we will discuss next. Moreover, a generalization of GPS signature scheme to superspecial abelian surfaces was proposed by Hao-Wei Chu in 2021 [Chu21, Appendix].

```
Signing $(p, \mathcal{B}, L, L', E_0, O_0, E_1, m, \mathsf{H}, \phi)$
$(\phi'_1, \dots, \phi'_t) \xleftarrow{\$} \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_1, -)^t$ of degree $L'$
$E'_i = \phi'_i(E_1),\ 1 \le i \le t$
$j'_i = j(E'_i),\ 1 \le i \le t$
$b \coloneqq \mathsf{H}(m, j'_1, \dots, j'_t)$
$\eta = (\eta_1, \dots, \eta_t)$
return $\sigma \coloneqq (b, \eta)$
```

```
Verification $(p, \mathcal{B}, L, L', E_0, O_0, E_1, m, \mathsf{H}, \sigma)$
$b_i = 0 \Rightarrow E'_i = \eta_i(E_1)\ 1 \le i \le t$
$b_i = 1 \Rightarrow E'_i = \eta_i(E_0)\ 1 \le i \le t$
$j'_i = j(E'_i)\ 1 \le i \le t$
return $b \overset{?}{=} \mathsf{H}(m, j'_1, \dots, j'_t)$
```

Figure 14: GPS signature scheme

3.2.2 SQISign (Short Quaternion and Isogeny Signature)

This signature scheme was introduced by Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski in 2020 [De +20]. The primary challenge in isogeny based signatures has been the development of a system with an exponentially large set of challenges, eliminating the need for repetition. This feat was accomplished by the creators of SQISign. Moreover, unlike GPS, this protocol has real life implementation[122] and an updated version of this scheme has also been submitted for standardization[123] under a new stylized name `SQIsign` [Cha+23].

Let λ be the security parameter. We fix a prime p such that the $N2^f$-torsion subgroup is defined over a small extension of $\mathbb{F}_{p^2}$ for smooth number $N \simeq p^{3/2}$ and f is as big as possible [De +20, §8.2] [Ler22, §5.4.2]. Let $N2^f = MM'$ such that M is a λ-bit integer consisting all the smallest factors, and M' is a 2λ-bit integer. Let $L = 2^e$, where e is greater than the diameter of $G_2(p)$ [De +20, §8.4] [Ler22, §5.4.3]. Moreover, we fix $E_0 : y^2 = x^3 + x$ in characteristic $p \equiv 3 \pmod 4$ with known special extremal endomorphism ring $O_0 \coloneqq \mathrm{End}_{\overline{\mathbb{F}}_p}(E_0)$, as we did for GPS protocol. The prover P chooses a random isogeny[124] $\phi : E_0 \to E_1$ such that $\deg(\phi)$ is a prime smaller than $2^{\lambda/2}$, leading to a random elliptic curve E_1. P keeps ϕ secret (witness/secret key) and publishes E_1 (public key). The verifier V knows p, E_0, $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_0)$, M, L, and E_1. But V doesn't know whether P knows $O_1 \coloneqq \mathrm{End}_{\overline{\mathbb{F}}_p}(E_1)$, or equivalently, a isogeny path $\phi : E_0 \to E_1$. Therefore, P can use the following Σ-protocol to prove knowledge of O_1 [Ler22, Lemma 5.2.1, Lemma 5.5.1]:

1. P generates a random (secret) M'-isogeny[125] walk $\phi' : E_0 \to E'_1$. P sends commitment E'_1 to V.

2. V sends the description of a cyclic M-isogeny[126] $\tau : E'_1 \to E'_2$ as challenge to P.

3. P sends an L-isogeny $\eta : E_1 \to E'_2$ as response to V, such that $\widehat{\tau} \circ \eta : E_1 \to E'_1$ is cyclic, computed[127] as follows:

   (a) *Isogeny to left O_1-ideal:* P computes the kernel[128] of τ, and then translates this kernel to ideal, obtaining kernel ideal I_τ from τ [Ler22, Algorithm 20 and p. 109]. Continuing this way, P computes left O_1-ideal $I \coloneqq \overline{I}_\phi \cdot I_{\phi'} \cdot I_\tau$ corresponding to the isogeny $\tau \circ \phi' \circ \widehat{\phi}$.

[122] On 28th February 2023, an interactive SageMath tutorial for SQISign was posted: `https://learningtosqi.github.io/`. Hence realizing Lorenz Panny's dream of having a toy SQISign implementation in SageMath [Pan22, Part 0: The Dream].

[123] Additional Digital Signature Candidates for the NIST PQC Standardization Process: `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`

[124] Since $\deg(\phi)$ is a large prime, we never compute the isogeny ϕ concretely, as this would be too inefficient. Instead, we use the corresponding ideal I_ϕ [Ler22, p. 136].

[125] With this choice of degree, computing the isogeny and converting it to an ideal is efficient.

[126] Since the MM'-torsion subgroup is defined over a small extension of $\mathbb{F}_{p^2}$, computing the corresponding ideal will be efficient.

[127] We need an isogeny that does not leak any information about ϕ. That is, $\eta \neq \tau \circ \phi' \circ \widehat{\phi}$ [De +20, §3.3].

[128] The perk of working with cyclic isogeny, which was not done in GPS.

(b) *Left O_1-ideal of norm L:* P uses the O_0O_1-ideal I_ϕ and left O_1-ideal I to generate a randomized left O_1-ideal $J \in [I]_{\mathsf{L}}$ of norm $L = 2^e$ [De +20, Algorithm 5] [Ler22, Algorithm 33].

(c) *Left O_1-ideal to isogeny:* P translates the left O_1-ideal J to kernel using various tricks, and then generates the desired L-isogeny $\eta : E_1 \to E_2'$ from the kernel [EHM17, Proposition 4.10, Definition 5.1] [Eis+18, Proposition 9, Definition 1] [De +20, §8.1] [Ler22, §4.2.2].

V checks if η is an L-isogeny from E_1 to E_2' such that $\hat{\tau} \circ \eta$ is a cyclic isogeny from E_1 to E_1'. To verify that $\widehat{\tau} \circ \eta$ is cyclic, it suffices to compute the action of $\widehat{\tau} \circ \eta$ on $E_1[2^f]$.

$$\begin{tikzcd}
E_0 \arrow[r, "\phi"] \arrow[d, "\phi'"'] & E_1 \arrow[d, squiggly, "\eta"'] \\
E_1' \arrow[r, dashed, "\tau"] & E_2'
\end{tikzcd}$$

This Σ-protocol is only computationally zero-knowledge based on an ad hoc assumption [Beu+23, §6.2]. Moreover, there exists some issues with the zero-knowledge of the first version of SQISign we discussed above [Ver23, p. 48]. Therefore, to fix such issues, some tweaks were made to the algorithms in an updated version of this scheme [De +23].

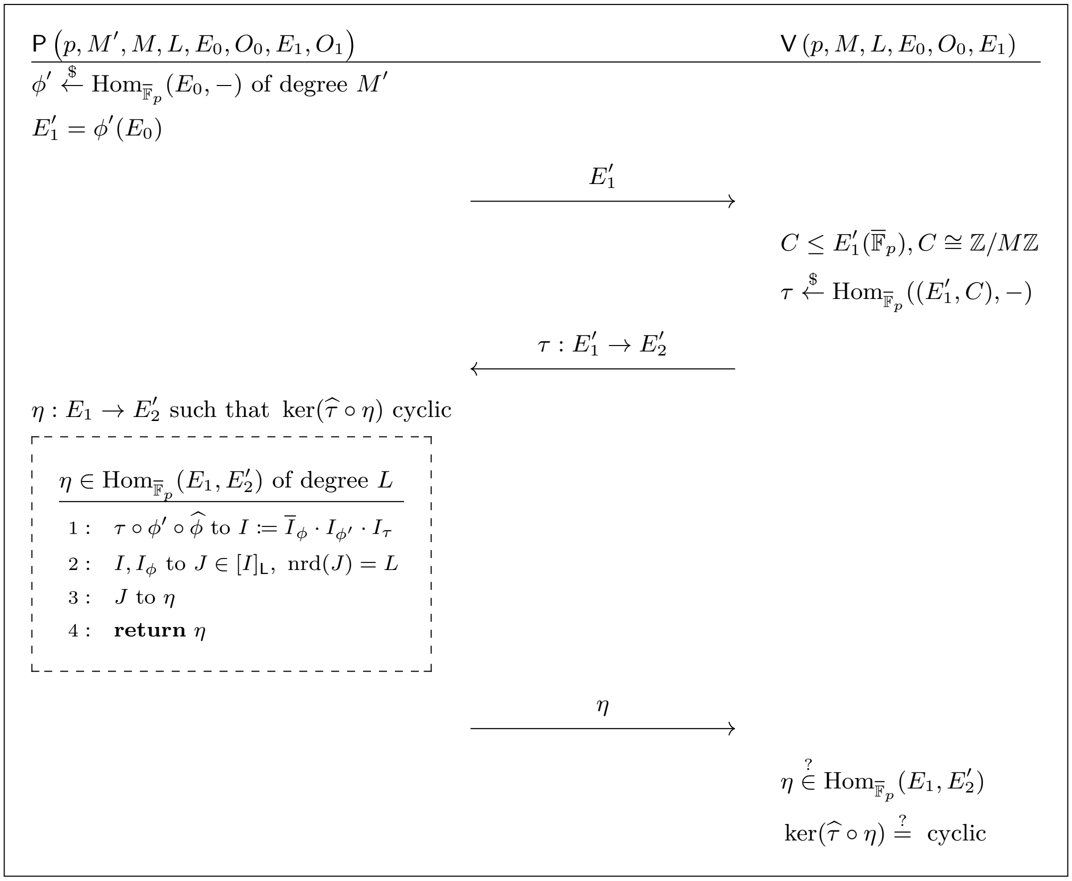

$\mathsf{P}\left(p, M', M, L, E_0, O_0, E_1, O_1\right)$
$\mathsf{V}\,(p, M, L, E_0, O_0, E_1)$
$\phi' \xleftarrow{\$} \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_0, -)$ of degree M'
$E_1' = \phi'(E_0)$
E_1'
$C \leq E_1'(\overline{\mathbb{F}}_p), C \cong \mathbb{Z}/M\mathbb{Z}$
$\tau \xleftarrow{\$} \mathrm{Hom}_{\overline{\mathbb{F}}_p}((E_1', C), -)$
$\tau : E_1' \to E_2'$
$\eta : E_1 \to E_2'$ such that $\ker(\widehat{\tau} \circ \eta)$ cyclic
$\eta \in \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_1, E_2')$ of degree L
1 : $\tau \circ \phi' \circ \widehat{\phi}$ to $I := \overline{I}_\phi \cdot I_{\phi'} \cdot I_\tau$
2 : I, I_ϕ to $J \in [I]_{\mathsf{L}}$, $\mathrm{nrd}(J) = L$
3 : J to η
4 : **return** η
η
$\eta \overset{?}{\in} \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_1, E_2')$
$\ker(\widehat{\tau} \circ \eta) \overset{?}{=}$ cyclic

Figure 15: SQISign Σ-protocol

Consider the same setup as for the SQISign identification protocol discussed above. Given the security parameter λ, the key generation algorithm G chooses a prime p such that the $N2^f$-torsion subgroup is defined over a small extension of $\mathbb{F}_{p^2}$ for smooth number $N \simeq p^{3/2}$ and f is as big as possible. Fix $N2^f = MM'$ such that M is a λ-bit integer consisting all the smallest factors, and M' is a 2λ-bit integer. Let $L = 2^e$, where

e is greater than the diameter of $G_2(p)$. Moreover, we fix $E_0 : y^2 = x^3 + x$ in characteristic $p \equiv 3 \pmod 4$ with known special extremal endomorphism ring $O_0 \coloneqq \mathrm{End}_{\overline{\mathbb{F}}_p}(E_0)$. Choose a random left O_0-ideal I_ϕ such that $\mathrm{nrd}(I_\phi)$ is a large prime smaller than $2^{\lambda/2}$. Compute another left O_0-ideal J_ϕ by solving quaternion 2^n-isogeny problem. Then the codomain of isogeny corresponding to J_ϕ is (public key) E_1 with (private key) $O_1 \coloneqq \mathrm{End}_{\overline{\mathbb{F}}_p}(E_1)$ [De +20, p. 41] [Ler22, p. 136]. Consider the (random oracle) cryptographic hash function $\mathsf{H} : \mathfrak{M} \times \mathfrak{A} \to \mathbb{Z} \cap [1, \psi(M)]$, where for $M = \prod_i \ell_i^{e_i}$ we have $\psi(M) = \prod_i \ell_i^{e_i - 1}(\ell_i + 1)$, $\mathfrak{A}$ is the set of j-invariants representing supersingular elliptic curves in characteristic p, and $\mathfrak{M}$ is the message space [De +20, §3.4] [Ler22, §5.2.2]. Here $\psi(M)$ is based on the compression algorithm [De +20, Algorithm 10] [Ler22, Algorithm 17, Lemma 4.1.3]. Now we can use Fiat-Shamir heuristics to transform the SQISign Σ-protocol into the following signature scheme [De +20, Theorem 2] [Ler22, Theorem 5.2.3]:

1. To sign a message $m \in \mathfrak{M}$, the signing algorithm randomly chooses M'-isogeny $\phi' : E_0 \to E_1'$, and computes $b \coloneqq \mathsf{H}(m, j(E_1'))$. Then it constructs an M-isogeny $\tau : E_1' \to E_2'$ using the decompression algorithm for the curve E_1', and integer b [De +20, Algorithm 11] [Ler22, Algorithm 18]. Finally, using secret key O_1 along with the isogeny $\tau \circ \phi' : E_0 \to E_2'$ it constructs a L-isogeny $\eta : E_1 \to E_2'$ such that $\widehat{\tau} \circ \eta$ is cyclic, to produce the signature $\sigma \coloneqq (E_1', \eta)$.

2. To verify the signature $\sigma = (E_1', \eta)$ on a message m using the public key E_1, the signature verification algorithm first computes $b = \mathsf{H}(m, j(E_1'))$ to recover $\tau : E_1' \to E_2'$ using the decompression algorithm and checks that η is an isogeny from E_1 to E_2' such that $\widehat{\tau} \circ \eta$ is cyclic.

```
Signing $(p, M', M, L, E_0, O_0, E_1, m, \mathsf{H}, O_1)$
$\phi' \xleftarrow{\$} \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_0, -)$ of degree $M'$
$E_1' = \phi'(E_0)$
$b \coloneqq \mathsf{H}(m, j(E_1'))$
$\tau \coloneqq \mathrm{Decompress}(E_1', b)$
$\eta : E_1 \to E_2',\ \deg(\eta) = L,\ \ker(\widehat{\tau} \circ \eta)$ cyclic
return $\sigma \coloneqq (E_1', \eta)$
```

```
Verification $(p, M, L, E_0, O_0, E_1, m, \mathsf{H}, \sigma)$
$b \coloneqq \mathsf{H}(m, j(E_1'))$
$\tau \coloneqq \mathrm{Decompress}(E_1', b)$
return $\eta \overset{?}{\in} \mathrm{Hom}_{\overline{\mathbb{F}}_p}(E_1, E_2')$ & $\ker(\widehat{\tau} \circ \eta) \overset{?}{=}$ cyclic
```

Figure 16: SQISign scheme

There is ongoing research focused on various aspects of this signature scheme, like finding suitable primes [CMN21] [Bru+23] [Cha+23, §5.2], analyzing security [Onu22] [Jac+23], and optimizing implementation [Lin+23] [Cor+23]. Moreover, another signature scheme called SQISignHD has been proposed that claims to leverage algorithmic breakthrough underlying the attack on SIDH to overcome the main drawbacks of SQISign [Dar+23].

> "Yes I have to repeatedly tell this to my students: to break a signature scheme you need to study the verification algorithm, not the signing algorithm"
> - Steven Galbraith (Aug 06, 2023), https://twitter.com/EllipticKiwi/status/1688271138072428544

Acknowledgement

My deepest gratitude goes to Craig Costello for his guidance and support throughout my work. I am very grateful to Kirti Joshi for overseeing the smooth progression of my degree and providing feedback on this report. I also appreciate David Glickenstein for his flexibility in granting deadline extensions, and Sazzadur Rahaman for helping me explore my interests in cryptography. I would also like to thank Douglas Ulmer and C. Douglas Haessig for their readiness and availability to serve on my committee.

I am indebted to Eda Kırımlı, Jana Sotáková, John Voight, Antonin Leroux, Sarah Arpin, Ricardo Acuña, David Lowry-Duda, Travis Morrison, and Hitesh Kumar for their valuable insights. The presentation here is partly influenced by the lectures of Alessandro Chiesa[129] [Tha22], Laura Geatti[130] [Sch08], Nadia Heninger[131], Tanja Lange[132] [Cas+18], Kristin Lauter[131] [CLG09], Hendrik Lenstra[131] [Len08], Francesco Pappalardi[130] [Men93], and René Schoof[130] [Sch82]. The illustrations in this report are made possible by the amazing work of SageMath contributors [The23].

References

[AAM19] Gora Adj, Omran Ahmadi, and Alfred Menezes. "On Isogeny Graphs of Supersingular Elliptic Curves over Finite Fields". In: *Finite Fields and Their Applications* 55 (2019), pp. 268–283. DOI: 10.1016/j.ffa.2018.10.002.

[AB04] Montserrat Alsina and Pilar Bayer. *Quaternion Orders, Quadratic Forms, and Shimura Curves.* Vol. 22. CRM Monograph Series. Providence, R.I: American Mathematical Society, 2004. 196 pp. DOI: 10.1090/crmm/022.

[Alu09] Paolo Aluffi. *Algebra: Chapter 0.* Vol. 104. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2009. xx+713. DOI: 10.1090/gsm/104.

[Amo+21] Laia Amorós et al. "Explicit Connections Between Supersingular Isogeny Graphs and Bruhat-Tits Trees". In: *Research Directions in Number Theory - Women in Numbers Europe III.* Vol. 24. Assoc. Women Math. Ser. Springer Cham, 2021, pp. 39–73. DOI: 10.1007/978-3-030-77700-5_2.

[Ara07] Donu Arapura. *A Pre-Introduction to Algebraic Geometry by Pictures.* 2007. URL: https://www.math.purdue.edu/~arapura/graph/algcurve.html.

[Ara12] Donu Arapura. "Abelian Varieties and Moduli". Lecture notes. Purdue University, 2012. URL: https://www.math.purdue.edu/~arapura/preprints/abelian.pdf.

[Ari19] Victor Manuel Aricheta. "Supersingular Elliptic Curves and Moonshine". In: *Symmetry, Integrability and Geometry: Methods and Applications* (Jan. 29, 2019). DOI: 10.3842/SIGMA.2019.007.

[Arp+21] Sarah Arpin et al. "Adventures in Supersingularland". In: *Experimental Mathematics* (2021), pp. 1–28. DOI: 10.1080/10586458.2021.1926009. Accompanying SageMath code: https://github.com/krstnmnlsn/Adventures-in-Supersingularland-Data.

[Arp+23] Sarah Arpin et al. "Orienteering with One Endomorphism". In: *La Matematica* 2.3 (2023), pp. 523–582. DOI: 10.1007/s44007-023-00053-2. Accompanying SageMath code: https://github.com/SarahArpin/WIN5.

[Arp22] Sarah Arpin. "Supersingular Elliptic Curve Isogeny Graphs". PhD thesis. Boulder, United States: University of Colorado at Boulder, 2022. 217 pp. URL: https://scholar.colorado.edu/concern/graduate_thesis_or_dissertations/2j62s6076.

[BA19] Sebastian Bozlee and Silviana Violet Amethyst. *Visualizing Complex Points of Elliptic Curves.* Illustrating Mathematics - ICERM Semester Program Fall 2019. Sept. 2019. URL: https://im.icerm.brown.edu/portfolio/visualizing-complex-points-of-elliptic-curves/.

[129] SLMath Summer Graduate School on Foundations and Frontiers of Probabilistic Proofs, Jul 17 - 28, 2023, Zürich, Switzerland. https://www.slmath.org/summer-schools/1037

[130] CIMPA/SEAMS School on Number Theory and Applications, Jun 12 - 22, 2023, Ho Chi Minh City, Vietnam. http://www.rnta.eu/HCMC2023/

[131] IAS/PCMI Graduate Summer School on Number Theory Informed by Computation, Jul 18 - Aug 05, 2022, Park City, United States. https://www.ias.edu/pcmi/pcmi-2022-summer-session

[132] IACR School on Applied Cryptography, Jan 30 - Feb 03, 2023, Bangkok, Thailand. https://sites.google.com/view/iacrschoolbkk2023

[Ban+19] Efrat Bank et al. “Cycles in the Supersingular ℓ-Isogeny Graph and Corresponding Endomorphisms”. In: *Research Directions in Number Theory - Women in Numbers IV*. Vol. 19. Assoc. Women Math. Ser. Springer Cham, 2019, pp. 41–66. DOI: 10.1007/978-3-030-19478-9_2.

[Bas+23] Andrea Basso et al. “Supersingular Curves You Can Trust”. In: *Advances in Cryptology – EUROCRYPT 2023*. Lecture Notes in Computer Science. Cham: Springer Nature Switzerland, 2023, pp. 405–437. DOI: 10.1007/978-3-031-30617-4_14.

[BD16] Gallen Ballew and James Duncan. *Arithmetic of elliptic curves*. Mathematical Computing Laboratory (MCL) project Spring 2016. University of Illinois at Chicago, 2016, p. 20. URL: https://mcl.math.uic.edu/mcl.math.uic.edu/wp-content/uploads/2016/05/S16-AEC-final-report.pdf. A video of 3D printing the torus representing an elliptic curve https://youtu.be/uPa48-V8T_4.

[Bel+09] Juliana Belding et al. “Computing Hilbert Class Polynomials”. In: *Algorithmic Number Theory*. Vol. 5011. Lecture Notes in Comput. Sci. Springer, Berlin, 2009, pp. 282–295. DOI: 10.1007/978-3-540-79456-1_19.

[Bel08] Juliana V. Belding. “Number Theoretic Algorithms For Elliptic Curves”. PhD thesis. College Park, United States: University of Maryland, College Park, 2008. URL: https://hdl.handle.net/1903/8456.

[Ben+23] Benjamin Benčina et al. *Improved Algorithms for Finding Fixed-Degree Isogenies between Supersingular Elliptic Curves*. 2023. URL: https://eprint.iacr.org/2023/1618. preprint.

[Ber+20] Daniel J. Bernstein et al. “Faster computation of isogenies of large prime degree”. In: *ANTS XIV – Fourteenth Algorithmic Number Theory Symposium*. Vol. 4. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2020, pp. 39–55. DOI: 10.2140/obs.2020.4.39. Sage implementation: https://velusqrt.isogeny.org/software.html.

[Bes+21] Alex J. Best et al. “Computing Classical Modular Forms”. In: *Arithmetic Geometry, Number Theory, and Computation*. Simons Symposia. Cham: Springer International Publishing, 2021, pp. 131–213. DOI: 10.1007/978-3-030-80914-0_4.

[Beu+23] Ward Beullens et al. “Proving Knowledge of Isogenies: A Survey”. In: *Designs, Codes and Cryptography*. Special Issue: Mathematics of Zero Knowledge 91.11 (2023), pp. 3425–3456. DOI: 10.1007/s10623-023-01243-3.

[BH12] Andries E. Brouwer and Willem H. Haemers. *Spectra of Graphs*. Universitext. New York, NY: Springer New York, 2012. DOI: 10.1007/978-1-4614-1939-6. Errata and addenda: https://homepages.cwi.nl/~aeb/math/ipm/.

[Bie89] Frédéric Bien. “Constructions of Telephone Networks by Group Representations”. In: *Notices of the American Mathematical Society* 36.1 (1989), pp. 5–22. URL: https://www.ams.org/journals/notices/198901/198901FullIssue.pdf.

[BLS12] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. “Modular Polynomials via Isogeny Volcanoes”. In: *Mathematics of Computation* 81.278 (2012), pp. 1201–1231. DOI: 10.1090/S0025-5718-2011-02508-1.

[BM23] Jennifer S. Balakrishnan and Barry Mazur. *Ogg’s Torsion conjecture: Fifty years later*. 2023. URL: http://arxiv.org/abs/2307.04752. This text is an expanded version of a 45-minute lecture that Mazur gave at the IAS on October 13, 2022: https://www.youtube.com/watch?v=RskabTDN2kw.

[BOS16] Jan Hendrik Bruinier, Ken Ono, and Andrew V. Sutherland. “Class Polynomials for Nonholomorphic Modular Functions”. In: *Journal of Number Theory* 161 (2016), pp. 204–229. DOI: 10.1016/j.jnt.2015.07.002.

[Brö09] Reinier Bröker. “Constructing Supersingular Elliptic Curves”. In: *Journal of Combinatorics and Number Theory* 1.3 (2009), pp. 269–273. URL: https://gkorpal.github.io/files/broker-supersingular.pdf.

[Bru+23] Giacomo Bruno et al. “Cryptographic Smooth Neighbors”. In: *To appear in the Proceedings of ASIACRYPT 2023*. Lecture Notes in Computer Science. Springer, 2023. URL: https://eprint.iacr.org/2022/1439. Accompanying C/C++ code: https://github.com/GiacomoBruno/TwinsmoothSearcher.

[Brz83] Juliusz Brzezinski. “On Orders in Quaternion Algebras”. In: *Communications in Algebra* 11.5 (1983), pp. 501–522. DOI: 10.1080/00927878308822861.

[BS23] Dan Boneh and Victor Shoup. “A Graduate Course in Applied Cryptography”. Book draft version 0.6. 2023. URL: https://toc.cryptobook.us/.

[BSS00] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Elliptic curves in cryptography.* Vol. 265. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2000. xvi+204. DOI: 10.1017/CBO9781107360211. Errata and addenda: https://nigelsmart.github.io/ECC/.

[Cas+18] Wouter Castryck et al. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology – ASIACRYPT 2018.* Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 395–427. DOI: 10.1007/978-3-030-03332-3_15. C implementation: https://csidh.isogeny.org/software.html.

[Cer04] J. M. Cerviño. "Supersingular Elliptic Curves and Maximal Quaternionic Orders". In: *Mathematisches Institut, Georg-August-Universität Göttingen: Seminars Summer Term 2004.* Universitätsdrucke Göttingen, Göttingen, 2004, pp. 53–60. URL: https://gkorpal.github.io/files/Cervino2004.pdf.

[CG14] Ilya Chevyrev and Steven D. Galbraith. "Constructing Supersingular Elliptic Curves with a given Endomorphism Ring". In: *LMS Journal of Computation and Mathematics* 17 (Special Issue A: Algorithmic Number Theory Symposium XI 2014), pp. 71–91. DOI: 10.1112/S1461157014000254.

[CGL08] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. "Families of Ramanujan Graphs and Quaternion Algebras". In: *Groups and Symmetries.* Vol. 47. CRM Proc. Lecture Notes. Amer. Math. Soc., Providence, RI, 2008, pp. 53–80. DOI: 10.1090/crmp/047/05.

[Cha+23] Jorge Chavez-Saab et al. *SQIsign: Algorithm Specifications and Supporting Documentation.* NIST Post-Quantum Cryptography: Additional Digital Signature Schemes Version 1.0. 2023, p. 67. URL: https://sqisign.org/.

[Cha23] Jasbir S. Chahal. "What Do Networks and Elliptic Curves Have in Common?" In: *American Mathematical Monthly* 130.2 (2023), pp. 158–175. DOI: 10.1080/00029890.2022.2141548.

[Chu21] Hao-Wei Chu. "Algorithms for Abelian Surfaces over Finite Fields and Their Applications to Cryptography". PhD thesis. State College, United States: The Pennsylvania State University, 2021. 122 pp. URL: https://etda.libraries.psu.edu/catalog/20786hzc5302.

[CL23] Giulio Codogni and Guido Lido. *Spectral Theory of Isogeny Graphs.* 2023. URL: http://arxiv.org/abs/2308.13913. preprint.

[Cla05] Pete L Clark. "Shimura Curves". Lecture notes for Math 726 - Introduction to Shimura Varieties. McGill University, 2005. URL: http://alpha.math.uga.edu/~pete/expositions2012.html.

[Cla15] Pete L Clark. "Commutative Algebra". Lecture notes. University of Georgia, 2015. URL: http://alpha.math.uga.edu/%7Epete/integral.pdf.

[CLG09] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. "Cryptographic Hash Functions from Expander Graphs". In: *Journal of Cryptology* 22.1 (2009), pp. 93–113. DOI: 10.1007/s00145-007-9002-x.

[CMN21] Craig Costello, Michael Meyer, and Michael Naehrig. "Sieving for Twin Smooth Integers with Solutions to the Prouhet-Tarry-Escott Problem". In: *Advances in Cryptology - EUROCRYPT 2021. Part I.* Vol. 12696. Lecture Notes in Comput. Sci. Springer, Cham, 2021, pp. 272–301. DOI: 10.1007/978-3-030-77870-5_10.

[Col22] Leonardo Colò. "Oriented Supersingular Elliptic Curves and Class Group Actions". PhD thesis. Marseille, France: Aix-Marseille Université, 2022. 281 pp. URL: http://www.theses.fr/2022AIXM0580.

[Con99] Ian Connell. "Elliptic Curve Handbook". Book draft. Montreal, 1999. URL: https://webs.ucm.es/BUCM/mat/doc8354.pdf.

[Cor+23] Maria Corte-Real Santos et al. "ApresSQI: Extra Fast Verification for SQIsign Using Extension-Field Signing". Preprint. 2023. URL: https://eprint.iacr.org/2023/1559. Accompanying SageMath implementation: https://github.com/TheSICQ/ApresSQI.

[Cos+19] Anamaria Costache et al. "Ramanujan Graphs in Cryptography". In: *Research Directions in Number Theory - Women in Numbers IV.* Vol. 19. Assoc. Women Math. Ser. Springer Cham, 2019, pp. 1–40. DOI: 10.1007/978-3-030-19478-9_1.

[Cos20] Craig Costello. "Supersingular Isogeny Key Exchange for Beginners". In: *Selected Areas in Cryptography – SAC 2019.* Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 21–50. DOI: 10.1007/978-3-030-38471-5_2.

[Cou96] AMS Council. "1996 Steele Prizes". In: *Notices of the American Mathematical Society* 43.11 (1996), pp. 1340–1347. URL: https://www.ams.org/notices/199611/comm-steele.pdf.

[Cow22] Alex Cowan. “Computing Newforms Using Supersingular Isogeny Graphs”. In: *Research in Number Theory (Topical collection: Algorithmic Number Theory Symposium XV)* 8.4 (Oct. 25, 2022), p. 96. DOI: 10.1007/s40993-022-00392-z.

[Cox22] David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* In collab. with Roger Lipsett. 3rd ed. AMS Chelsea Publishing, Providence, RI, 2022. xv+533. DOI: 10.1090/chel/387. Errata and addenda: https://dacox.people.amherst.edu/primes.html.

[CPV20] Wouter Castryck, Lorenz Panny, and Frederik Vercauteren. “Rational Isogenies from Irrational Endomorphisms”. In: *Advances in Cryptology – EUROCRYPT 2020.* Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 523–548. DOI: 10.1007/978-3-030-45724-2_18.

[Cra97] Ronald John Fitzgerald Cramer. “Modular Design of Secure yet Practical Cryptographic Protocols”. PhD thesis. Amsterdam, Netherlands: University of Amsterdam, 1997. URL: https://ir.cwi.nl/pub/21438.

[Cre19] Richard Crew. “Local Class Field Theory”. Lecture notes. University of Florida, 2019. URL: https://people.clas.ufl.edu/rcrew/files/LCFT.pdf.

[Dam10] Ivan Damgård. *On Σ-protocols.* 2010. URL: https://www.cs.au.dk/~ivan/Sigma.pdf.

[Dar+23] Pierrick Dartois et al. *SQISignHD: New Dimensions in Cryptography.* 2023. URL: https://eprint.iacr.org/2023/436. preprint.

[Dar04] Henri Darmon. *Rational Points on Modular Elliptic Curves.* Vol. 101. CBMS Reg. Conf. Ser. Math. Providence, RI: American Mathematical Society (AMS), 2004. URL: https://www.math.mcgill.ca/darmon/pub/Articles/Research/36.NSF-CBMS/chapter.pdf.

[Dar09] Henri Darmon. “Rational Points on Curves”. In: *Arithmetic Geometry.* Vol. 8. Clay Math. Proc. Amer. Math. Soc., Providence, RI, 2009, pp. 7–53. URL: https://www.claymath.org/library/proceedings/cmip08c.pdf.

[DDT95] Henri Darmon, Fred Diamond, and Richard Taylor. “Fermat’s Last Theorem”. In: *Current Developments in Mathematics.* Vol. 1995. International Press of Boston, Inc., 1995, pp. 1–154. DOI: 10.4310/CDM.1995.v1995.n1.a1.

[De +20] Luca De Feo et al. “SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies”. In: *Advances in Cryptology – ASIACRYPT 2020.* Vol. 12491. Cham: Springer International Publishing, 2020, pp. 64–93. DOI: 10.1007/978-3-030-64837-4_3. Extended version: https://eprint.iacr.org/2020/1240.

[De +23] Luca De Feo et al. “New Algorithms for the Deuring Correspondence: Towards Practical and Secure SQISign Signatures”. In: *Advances in Cryptology – EUROCRYPT 2023.* Lecture Notes in Comput. Sci. Springer, Cham, 2023, pp. 659–690. DOI: 10.1007/978-3-031-30589-4_23. Accompanying implementation in C: https://github.com/SQISign/sqisign-ec23.

[Déc98] Isabelle Déchène. “Quaternion Algebras and the Graph Method for Elliptic Curves”. MSc thesis. Montreal, Canada: McGill University, 1998. URL: https://escholarship.mcgill.ca/concern/theses/rj430682d.

[Del75] Pierre Deligne. “Courbes Elliptiques: Formulaire d’après J. Tate”. In: *Modular Functions of One Variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972).* Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975, pp. 53–73. DOI: 10.1007/BFb0097583.

[Deu41] Max Deuring. “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper”. In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 14.1 (1941), pp. 197–272. DOI: 10.1007/BF02940746.

[DG16] Christina Delfs and Steven D. Galbraith. “Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$”. In: *Designs, Codes and Cryptography* 78.2 (Feb. 1, 2016), pp. 425–440. DOI: 10.1007/s10623-014-0010-1.

[DI95] Fred Diamond and John Im. “Modular Forms and Modular Curves”. In: *Seminar on Fermat’s Last Theorem (Toronto, ON, 1993–1994).* Vol. 17. CMS Conf. Proc. Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. URL: https://wstein.org/edu/Fall2003/252/references/diamond-im/.

[DJP14] Luca De Feo, David Jao, and Jérôme Plût. “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies”. In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247. DOI: 10.1515/jmc-2012-0015.

[DR73] Pierre Deligne and Michael Rapoport. “Les Schémas de Modules de Courbes Elliptiques”. In: *Modular Functions of One Variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973, pp. 143–316. DOI: 10.1007/978-3-540-37855-6_4.

[DS12] Della Dumbaugh and Joachim Schwermer. “The Collaboration of Emil Artin and George Whaples: Artin’s Mathematical Circle Extends to America”. In: *Archive for History of Exact Sciences* 66.5 (2012), pp. 465–484. DOI: 10.1007/s00407-012-0100-2.

[DS16] Fred Diamond and Jerry M. Shurman. *A First Course in Modular Forms*. corrected 4th printing. Vol. 228. Graduate Texts in Mathematics. New York: Springer, 2016. 450 pp. DOI: 10.1007/978-0-387-27226-9.

[DSV03] Giuliana Davidoff, Peter Sarnak, and Alain Valette. *Elementary Number Theory, Group Theory, and Ramanujan Graphs*. Vol. 55. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 2003. x+144. DOI: 10.1017/CBO9780511615825.

[EHM17] Kirsten Eisenträger, Sean Hallgren, and Travis Morrison. *On the Hardness of Computing Endomorphism Rings of Supersingular Elliptic Curves*. 2017. URL: https://eprint.iacr.org/2017/986. preprint.

[Eis+18] Kirsten Eisenträger et al. “Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions”. In: *Advances in Cryptology – EUROCRYPT 2018*. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 329–368. DOI: 10.1007/978-3-319-78372-7_11.

[Eis+20] Kirsten Eisenträger et al. “Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs”. In: *ANTS XIV – Fourteenth Algorithmic Number Theory Symposium*. Vol. 4. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2020, pp. 215–232. DOI: 10.2140/obs.2020.4.215. Accompanying SageMath code: https://github.com/travismo/bass-experiments.

[Elk87] Noam D. Elkies. “The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$”. In: *Inventiones mathematicae* 89.3 (Oct. 1, 1987), pp. 561–567. DOI: 10.1007/BF01388985.

[Elk91] Noam D. Elkies. “Distribution of Supersingular Primes”. In: *Journées Arithmétiques de Luminy 17-21 Juillet 1989*. Astérisque. Société mathématique de France, 1991. URL: http://www.numdam.org/item/AST_1991__198-199-200__127_0/.

[Elk98] Noam D. Elkies. “Elliptic and Modular Curves over Finite Fields and Related Computational Issues”. In: *Computational Perspectives on Number Theory (Chicago, IL, 1995)*. Vol. 7. AMS/IP Stud. Adv. Math. Amer. Math. Soc., Providence, RI, 1998, pp. 21–76. DOI: 10.1090/amsip/007/03.

[Eme02] Matthew Emerton. “Supersingular Elliptic Curves, Theta Series and Weight Two Modular Forms”. In: *Journal of the American Mathematical Society* 15.3 (2002), pp. 671–714. DOI: 10.1090/S0894-0347-02-00390-9.

[Eng99] Andreas Enge. *Elliptic Curves and Their Applications to Cryptography*. 1st ed. New York, NY: Springer US, 1999. DOI: 10.1007/978-1-4615-5207-9.

[Eri+23] Jonathan Komada Eriksen et al. “Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic”. In: *To appear in the Proceedings of LMFDB, Computation, and Number Theory (LuCaNT)*. Contemporary Mathematics. Amer. Math. Soc., Providence, R.I., 2023. URL: https://lucant.org/papers/230122-Panny.pdf. Accompanying SageMath code: https://github.com/friends-of-quaternions/deuring.

[EvdGM08] Bas Edixhoven, Gerard van der Geer, and Ben Moonen. “Modular Forms”. In: *Modular Forms on Schiermonnikoog*. Cambridge Univ. Press, Cambridge, 2008, pp. 1–11. DOI: 10.1017/CBO9780511543371.002.

[FH99] Masahiro Furumoto and Yuji Hasegawa. “Hyperelliptic Quotients of Modular Curves $X_0(N)$”. In: *Tokyo Journal of Mathematics* 22.1 (1999), pp. 105–125. DOI: 10.3836/tjm/1270041616.

[FM14] Cameron Franc and Marc Masdeu. “Computing fundamental domains for the Bruhat-Tits tree for $GL_2(\mathbb{Q}_p)$, p-adic automorphic forms, and the canonical embedding of Shimura curves”. In: *LMS Journal of Computation and Mathematics* 17.1 (2014), pp. 1–23. DOI: 10.1112/S1461157013000235. https://doc.sagemath.org/html/en/reference/modsym/sage/modular/btquotients/btquotient.html.

[FM99] Gerhard Frey and Michael Müller. “Arithmetic of Modular Curves and Applications”. In: *Algorithmic Algebra and Number Theory*. Berlin, Heidelberg: Springer, 1999, pp. 11–48. DOI: 10.1007/978-3-642-59932-3_2.

[Fus+23] Jenny Fuselier et al. “Computing supersingular endomorphism rings using inseparable endomorphisms”. Preprint. 2023. URL: http://arxiv.org/abs/2306.03051. Accompanying SageMath code: https://github.com/travismo/inseparables.

[Gal01] Steven D. Galbraith. “Supersingular Curves in Cryptography”. In: *Advances in Cryptology — ASIACRYPT 2001*. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2001, pp. 495–513. DOI: 10.1007/3-540-45682-1_29.

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. 1st ed. 2012. DOI: 10.1017/CBO9781139012843. Errata and addenda: https://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html.

[Gal96] Steven D. Galbraith. “Equations for Modular Curves”. PhD thesis. Oxford, England: University of Oxford, 1996. URL: https://ora.ox.ac.uk/objects/uuid:4b893bc3-f4fe-4877-872a-6a7dd4d5c76d.

[Gal99] Steven D. Galbraith. “Constructing Isogenies between Elliptic Curves over Finite Fields”. In: *LMS Journal of Computation and Mathematics* 2 (1999), pp. 118–138. DOI: 10.1112/S1461157000000097.

[Gol01] Oded Goldreich. *Foundations of Cryptography: Volume 1: Basic Tools*. Vol. 1. Cambridge: Cambridge University Press, 2001. DOI: 10.1017/CBO9780511546891.

[GPS20] Steven D. Galbraith, Christophe Petit, and Javier Silva. “Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems”. In: *Journal of Cryptology* 33.1 (2020), pp. 130–175. DOI: 10.1007/s00145-019-09316-0.

[Gro87] Benedict H. Gross. “Heights and the special values of L-series”. In: *Number theory (Montreal, Que., 1985)*. Vol. 7. CMS Conf. Proc. Amer. Math. Soc., Providence, RI, 1987, pp. 115–187. URL: https://wstein.org/papers/bib/Gross-Heights_and_the_Special_Values_of_L-series.pdf.

[GS13] Steven Galbraith and Anton Stolbunov. “Improved Algorithm for the Isogeny Problem for Ordinary Elliptic Curves”. In: *Applicable Algebra in Engineering, Communication and Computing* 24.2 (2013), pp. 107–131. DOI: 10.1007/s00200-013-0185-0.

[GS17] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*. 2nd ed. Cambridge Studies in Advanced Mathematics. Cambridge: Cambridge University Press, 2017. DOI: 10.1017/9781316661277.

[Gul20] Daniel Gulotta. *Ramanujan Graphs, Quaternions, and Number Theory*. Canada/USA Mathcamp, 2020. URL: https://dgulotta.github.io/mc20.html.

[GV11] Matthew Greenberg and John Voight. “Computing Systems of Hecke Eigenvalues Associated to Hilbert Modular Forms”. In: *Mathematics of Computation* 80.274 (2011), pp. 1071–1092. DOI: 10.1090/S0025-5718-2010-02423-8.

[GV18] Steven D. Galbraith and Frederik Vercauteren. “Computational Problems in Supersingular Elliptic Curve Isogenies”. In: *Quantum Information Processing* 17.10 (2018), Paper No. 265, 22. DOI: 10.1007/s11128-018-2023-6.

[Haj23] Nadir Hajouji. *Supersingular Isogeny Graphs from Algebraic Modular Curves*. 2023. URL: http://arxiv.org/abs/2303.09096. preprint.

[Has80] Ki-Ichiro Hashimoto. “Some Examples of Integral Definite Quaternary Quadratic Forms with Prime Discriminant”. In: *Nagoya Mathematical Journal* 77 (Feb. 1980), pp. 167–175. DOI: 10.1017/S0027763000018742.

[Has95] Ki-ichiro Hashimoto. “Explicit Form of Quaternion Modular Embeddings”. In: *Osaka Journal of Mathematics* 32.3 (1995), pp. 533–546. DOI: 10.18910/11970.

[Has97] Yuji Hasegawa. “Hyperelliptic modular curves $X_0^*(N)$”. In: *Acta Arithmetica* 81 (1997), pp. 369–385. DOI: 10.4064/aa-81-4-369-385.

[HH96] Yuji Hasegawa and Ki-ichiro Hashimoto. “Hyperelliptic modular curves $X_0^*(N)$ with square-free levels”. In: *Acta Arithmetica* 77.2 (1996), pp. 179–193. DOI: 10.4064/aa-77-2-179-193.

[HK04] Hans-Jürgen Hoehnke and Max-Albert Knus. “Algebras, Their Invariants and K-forms: A Tribute to [the Work of] HEINRICH BRANDT on the 50th Anniversary of His Death”. Lecture notes. ETH Zürich, 2004. URL: https://people.math.ethz.ch/~knus/papers/brandt04.pdf.

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. “Expander Graphs and Their Applications”. In: *Bulletin of the American Mathematical Society* 43.4 (2006), pp. 439–561. DOI: 10.1090/S0273-0979-06-01126-8.

[HM98] Joe Harris and Ian Morrison. *Moduli of Curves*. Vol. 187. Graduate Texts in Mathematics. Springer-Verlag, New York, 1998. xiv+366. DOI: 10.1007/b98867.

[HPS14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. Second. Undergraduate Texts in Mathematics. Springer, New York, 2014. xviii+538. DOI: 10.1007/978-1-4939-1711-2.

[Hus04] Dale Husemöller. *Elliptic Curves*. 2nd ed. Graduate Texts in Mathematics 111. New York: Springer, 2004. 487 pp. DOI: 10.1007/b97292.

[Ibu82] Tomoyoshi Ibukiyama. "On Maximal Orders of Division Quaternion Algebras over the Rational Number Field with Certain Optimal Embeddings". In: *Nagoya Mathematical Journal* 88 (1982), pp. 181–195. DOI: 10.1017/S002776300002016X.

[Igu58] Jun-ichi Igusa. "Class Number of a Definite Quaternion with Prime Discriminant". In: *Proceedings of the National Academy of Sciences of the United States of America* 44 (1958), pp. 312–314. DOI: 10.1073/pnas.44.4.312.

[Igu59] Jun-ichi Igusa. "Kroneckerian Model of Fields of Elliptic Modular Functions". In: *Amer. J. Math.* 81 (1959), pp. 561–577. DOI: 10.2307/2372914.

[Inc23] OEIS Foundation Inc. *The On-Line Encyclopedia of Integer Sequences*. 2023. URL: https://oeis.org/.

[Jac+23] David Jacquemin et al. *Towards a Constant-Time Implementation of Isogeny-Based Signature, SQISign*. 2023. URL: https://eprint.iacr.org/2023/807. preprint.

[Jao03] David Jao. "Supersingular Primes for Rational Points on Modular Curves". PhD thesis. Massachusetts, United States: Harvard University, 2003. 88 pp. URL: https://www.proquest.com/docview/305334030/abstract/C4BB3C1E9F004B6FPQ/1.

[JMV05] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. "Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?" In: *Advances in Cryptology - ASIACRYPT 2005*. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2005, pp. 21–40. DOI: 10.1007/11593447_2.

[Ken20] Autumn Kent. *Exploring the World of Atari, Doughnuts and Geometry*. College of Letters & Science, University of Wisconsin, Madison. May 4, 2020. URL: https://ls.wisc.edu/news/exploring-the-world-of-atari-doughnuts-and-geometry.

[Ken21] Keith Kendig. *A Gateway to Number Theory: Applying the Power of Algebraic Curves*. Vol. 57. The Dolciani Mathematical Expositions. MAA Press, Providence, RI; American Mathematical Society, Providence, RI, 2021. xv+207. DOI: 10.1090/dol/057.

[Ken77] Monsur A. Kenku. "Atkin-Lehner Involutions and Class Number Residuality". In: *Acta Arithmetica* 33.1 (1977), pp. 1–9. DOI: 10.4064/aa-33-1-1-9.

[KKS11] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito. *Number Theory 2: Introduction to Class Field Theory*. Trans. by Masato Kuwata and Katsumi Nomizu. Vol. 240. Translations of Mathematical Monographs. Providence: American Mathematical Society, 2011. viii+240. DOI: 10.1090/mmono/240.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves*. Vol. 108. Annals of Mathematics Studies. Princeton University Press, Princeton, NJ, 1985. xiv+514. DOI: 10.1515/9781400881710.

[Kob82] Neal Koblitz. "Why Study Equations over Finite Fields?" In: *Mathematics Magazine* 55.3 (1982), pp. 144–149. DOI: 10.2307/2690080.

[Koh+14] David R. Kohel et al. "On the quaternion ℓ-isogeny path problem". In: *LMS Journal of Computation and Mathematics* 17 (Special Issue A: Algorithmic Number Theory Symposium XI 2014), pp. 418–432. DOI: 10.1112/S1461157014000151.

[Koh01] David R. Kohel. "Hecke Module Structure of Quaternions". In: *Class Field Theory—Its Centenary and Prospect (Tokyo, 1998)*. Vol. 30. Adv. Stud. Pure Math. Math. Soc. Japan, Tokyo, 2001, pp. 177–195. DOI: 10.2969/aspm/03010177.

[Koh96] David R. Kohel. "Endomorphism Rings of Elliptic Curves over Finite Fields". PhD thesis. Berkley, United States: University of California, Berkeley, 1996. 117 pp. URL: http://www.i2m.univ-amu.fr/perso/david.kohel/pub/thesis.pdf.

[Koh97] David R. Kohel. "Computing Modular Curves via Quaternions". Notes from a talk given at the fourth CANT conference. Sydney, Australia, 1997. URL: https://wstein.org/papers/bib/kohel-sydney.pdf.

[KV10] Markus Kirschmer and John Voight. "Algorithmic Enumeration of Ideal Classes for Quaternion Orders". In: *SIAM Journal on Computing* 39.5 (Jan. 2010), pp. 1714–1747. DOI: 10.1137/080734467. Corrigendum available at https://doi.org/10.1137/120866063.

[Lan87] Serge Lang. *Elliptic Functions*. 2nd ed. Vol. 112. Graduate Texts in Mathematics. New York, NY: Springer New York, 1987. DOI: 10.1007/978-1-4612-4752-4.

[LB20] Jonathan Love and Dan Boneh. "Supersingular Curves with Small Noninteger Endomorphisms". In: *ANTS XIV – Fourteenth Algorithmic Number Theory Symposium*. Vol. 4. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2020, pp. 7–22. DOI: 10.2140/obs.2020.4.7.

[Lem11a] Franz Lemmermeyer. *Parametrizing Algebraic Curves*. Aug. 31, 2011. URL: http://arxiv.org/abs/1108.6219. preprint.

[Lem11b] Stefan Lemurell. "Quaternion Orders and Ternary Quadratic Forms". 2011. URL: https://arxiv.org/abs/1103.4922. Originally appeared as part of the authors Ph.D. thesis in 1997 (whose name then was Stefan Johansson) under the title "A Description of Quaternion Algebras".

[Len08] Hendrik W. Lenstra. "Lattices". In: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*. Vol. 44. Math. Sci. Res. Inst. Publ. Cambridge Univ. Press, Cambridge, 2008, pp. 127–181. URL: https://www.math.leidenuniv.nl/~psh/ANTproc/06hwl.pdf.

[Ler22] Antonin Leroux. "Quaternion Algebras and Isogeny-Based Cryptography". PhD thesis. Paris, France: École Polytechnique, 2022. 199 pp. URL: https://inria.hal.science/tel-03886810.

[Li96] Wen-Ching Winnie Li. *Number Theory with Applications*. Vol. 7. Series on University Mathematics. World Scientific Publishing Co., Inc., River Edge, NJ, 1996. xii+229. DOI: 10.1142/2716.

[Lin+23] Kaizhan Lin et al. *A Faster Software Implementation of SQISign*. 2023. URL: https://eprint.iacr.org/2023/753. preprint.

[Liu06] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics. Oxford University Press, 2006. Errata and addenda: https://www.math.u-bordeaux.fr/~qliu/Book/.

[Liv01] Ron Livné. "Communication Networks and Hilbert Modular Forms". In: *Applications of Algebraic Geometry to Coding Theory, Physics and Computation*. NATO Science Series. Dordrecht: Springer Netherlands, 2001, pp. 255–270. DOI: 10.1007/978-94-010-1011-5_13.

[LM04] Kristin Lauter and Ken McMurdy. *Explicit Generators for Endomorphism Rings of Supersingular Elliptic Curves*. 2004. URL: https://phobos.ramapo.edu/~kmcmurdy/research/ss_endomorphisms.pdf. preprint.

[Loe14] David Loeffler. "Modular Curves". Lecture notes for Taught Course Centre 2014. University of Warwick, 2014. URL: https://warwick.ac.uk/fac/sci/maths/people/staff/david_loeffler/teaching/modularcurves/lecture_notes.pdf.

[LOX20] Songsong Li, Yi Ouyang, and Zheng Xu. "Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$". In: *Finite Fields and Their Applications* 62 (2020). DOI: 10.1016/j.ffa.2019.101619.

[Loz11] Álvaro Lozano-Robledo. *Elliptic Curves, Modular Forms, and Their L-functions*. Vol. 58. Student Mathematical Library (IAS/Park City Mathematical Subseries). American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ, 2011. xiv+195. DOI: 10.1090/stml/058.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. "Ramanujan Graphs". In: *Combinatorica* 8.3 (1988), pp. 261–277. DOI: 10.1007/BF02126799.

[Mar14] Kimball Martin. "Graph Theory and Social Networks". Lecture notes for Math 4673/5673 - Graph Theory I. University of Oklahoma, 2014. URL: http://www2.math.ou.edu/~kmartin/graphs/.

[Mar17] Kimball Martin. "Quaternion Algebras in Number Theory". Lecture notes for Math 6393. University of Oklahoma, 2017. URL: https://math.ou.edu/~kmartin/quaint/.

[Maz77] Barry Mazur. "Modular Curves and the Eisenstein Ideal". In: *Institut des Hautes Études Scientifiques. Publications Mathématiques* 47 (1977). In collab. with Michael Rapoport, 33–186 (1978). URL: http://www.numdam.org/item/?id=PMIHES_1977__47__33_0.

[Maz78] Barry Mazur. "Rational Isogenies of Prime Degree". In: *Inventiones Mathematicae* 44.2 (1978). In collab. with Dorian M. Goldfeld, pp. 129–162. DOI: 10.1007/BF01390348.

[McM14] Ken McMurdy. *Explicit Representation of the Endomorphism Rings of Supersingular Elliptic Curves*. 2014. URL: https://phobos.ramapo.edu/~kmcmurdy/research/McMurdy-ssEndoRings.pdf. preprint.

[Men93] Alfred Menezes. *Elliptic Curve Public Key Cryptosystems*. 1st ed. Vol. 234. Series in Engineering and Computer Science. New York: Springer US, 1993. DOI: 10.1007/978-1-4615-3198-2.

[Mes86] Jean-François Mestre. "La méthode des graphes. Exemples et applications". In: *International conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*. In collab. with Joseph Oesterlé. Nagoya Univ., Nagoya, 1986, pp. 217–242. URL: https://wstein.org/msri06/refs/mestre-method-of-graphs/Mestre-La_Method_de_Graphes.pdf. English translation by Andrei Jorza: https://wstein.org/msri06/refs/mestre-method-of-graphs/mestre-en.pdf.

[Mil21] James S. Milne. *Elliptic Curves*. 2nd ed. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2021. x+308. doi: 10.1142/11870.

[Mir95] Rick Miranda. *Algebraic Curves and Riemann Surfaces*. Vol. 5. Graduate Studies in Mathematics. Providence, Rhode Island: American Mathematical Society, Apr. 17, 1995. doi: 10.1090/gsm/005.

[Mor08] Patrick Morton. *Ogg's Theorem via Explicit Congruences for Class Equations*. 2008. IUPUI Math Dept. Preprint Series: PR06-09. url: https://web.archive.org/web/20100629154932/http://www.math.iupui.edu/research/preprint/2006/pr06-09.pdf. preprint.

[Mor91] Carlos Moreno. *Algebraic Curves over Finite Fields*. Vol. 97. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 1991. x+246. doi: 10.1017/CBO9780511608766.

[MP19] Chloe Martindale and Lorenz Panny. "Isogeny-Based Cryptography". In: *Computeralgebra-Rundbrief* 65 (2019), pp. 12–17. url: https://fachgruppe-computeralgebra.de/data/CA-Rundbrief/car65.pdf.

[MS74] Barry Mazur and Peter Swinnerton-Dyer. "Arithmetic of Weil Curves". In: *Inventiones mathematicae* 25.1 (1974), pp. 1–61. doi: 10.1007/BF01389997.

[MT93] Carlos Munuera and Juan G. Tena. "An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite field". In: *Rendiconti del Circolo Matematico di Palermo* 42.1 (1993), pp. 106–116. doi: 10.1007/BF02845114.

[Mur92] Naoki Murabayashi. "On Normal Forms of Modular Curves of Genus 2". In: *Osaka Journal of Mathematics* 29.2 (1992), pp. 405–418. doi: 10.18910/8956.

[MW23] Arthur Herlédan Le Merdy and Benjamin Wesolowski. *The Supersingular Endomorphism Ring Problem given One Endomorphism*. 2023. url: http://arxiv.org/abs/2309.11912. preprint.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Trans. by Norbert Schappacher. Vol. 322. Grundlehren Der Mathematischen Wissenschaften. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999. doi: 10.1007/978-3-662-03983-0.

[NG22] Anil Nerode and Noam Greenberg. *Algebraic Curves and Riemann Surfaces for Undergraduates: The Theory of the Donut*. 1st ed. Cham: Springer, 2022. doi: 10.1007/978-3-031-11616-2.

[NN01] Raghavan Narasimhan and Yves Nievergelt. *Complex Analysis in One Variable*. 2nd ed. Boston, MA: Birkhäuser Boston, 2001. doi: 10.1007/978-1-4612-0175-5.

[Ogg74] Andrew P. Ogg. "Hyperelliptic Modular Curves". In: *Bulletin de la Société Mathématique de France* 102 (1974), pp. 449–462. doi: 10.24033/bsmf.1789.

[Ogg75a] Andrew P. Ogg. "Automorphismes de courbes modulaires". In: *Séminaire Delange-Pisot-Poitou. Théorie des nombres* 16.1 (1975), pp. 1–8. url: http://www.numdam.org/item/SDPP_1974-1975__16_1_A4_0/.

[Ogg75b] Andrew P. Ogg. "Diophantine Equations and Modular Forms". In: *Bulletin of the American Mathematical Society* 81 (1975), pp. 14–27. doi: 10.1090/S0002-9904-1975-13623-8.

[Ogg80] Andrew P. Ogg. "Modular Functions". In: *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*. Vol. 37. Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, R.I., 1980, pp. 521–532. doi: 10.1090/pspum/037/604631.

[Onu22] Hiroshi Onuki. "On the Key Generation in SQISign". Lecture notes for NuTMiC 2022. Adam Mickiewicz University, Poznań, Poland, 2022. url: https://eprint.iacr.org/2022/900.

[OS16] Frans Oort and Norbert Schappacher. "Early History of the Riemann Hypothesis in Positive Characteristic". In: *The Legacy of Bernhard Riemann after One Hundred and Fifty Years. Vol. II*. Vol. 35. Adv. Lect. Math. (ALM). Int. Press, Somerville, MA, 2016, pp. 595–631. url: https://webspace.science.uu.nl/~oort0109/EigArt-HistpRH-2016.pdf.

[Pan21] Lorenz Panny. "Cryptography on Isogeny Graphs". PhD thesis. Eindhoven, Netherlands: Technische Universiteit Eindhoven, 2021. url: https://research.tue.nl/en/publications/cryptography-on-isogeny-graphs.

[Pan22] Lorenz Panny. "Isogenies in SageMath: Past, Present, Future". Presentation at Leuven Isogeny Days 3 (ISOCRYPT) (KU Leuven). Oct. 25, 2022. url: https://yx7.cc/docs/sage/sageisog_leuven_slides.pdf. The video recording is available here https://www.youtube.com/watch?v=itwTMmiPPew.

[Piz78] Arnold K. Pizer. "A Note on a Conjecture of Hecke". In: *Pacific Journal of Mathematics* 79.2 (Jan. 1978), pp. 541–548. url: https://projecteuclid.org/journals/pacific-journal-of-mathematics/volume-79/issue-2/A-note-on-a-conjecture-of-Hecke/pjm/1102805800.full.

[Piz80] Arnold K. Pizer. "An algorithm for computing modular forms on $\Gamma_0(N)$". In: *Journal of Algebra* 64.2 (1980), pp. 340–390. DOI: 10.1016/0021-8693(80)90151-9.

[Piz90] Arnold K. Pizer. "Ramanujan Graphs and Hecke Operators". In: *Bulletin of the American Mathematical Society* 23.1 (1990), pp. 127–137. DOI: 10.1090/S0273-0979-1990-15918-X.

[Piz98] Arnold K. Pizer. "Ramanujan graphs". In: *Computational perspectives on number theory (Chicago, IL, 1995)*. Vol. 7. AMS/IP Stud. Adv. Math. Amer. Math. Soc., Providence, RI, 1998, pp. 159–178. DOI: 10.1090/amsip/007/08. Scan of the paper: https://gkorpal.github.io/files/pizer.pdf.

[PL17] Christophe Petit and Kristin Lauter. *Hard and Easy Problems for Supersingular Isogeny Graphs*. 2017. URL: https://eprint.iacr.org/2017/962. preprint.

[PS18] Christophe Petit and Spike Smith. "An improvement to the quaternion analogue of the ℓ-isogeny path problem". Presentation at MathCrypt 2018 (extended abstract). MathCrypt (Santa Barbara). 2018. URL: https://crypto.iacr.org/2018/affevents/mathcrypt/medias/08-50_3.pdf.

[PW23] Aurel Page and Benjamin Wesolowski. *The Supersingular Endomorphism Ring and One Endomorphism Problems Are Equivalent*. 2023. URL: https://arxiv.org/abs/2309.10432. preprint.

[Ray18] Dimitrij Ray. "Constructing the Deuring correspondence with applications to supersingular isogeny-based cryptography". MSc thesis. Eindhoven, Netherlands: Eindhoven University of Technology, 2018. 43 pp. URL: https://research.tue.nl/en/studentTheses/fb259177-cdba-44ce-bb67-4b45de5d8776.

[RB12] Adrian Rice and Ezra Brown. "Why Ellipses Are Not Elliptic Curves". In: *Mathematics Magazine* 85.3 (2012), pp. 163–176. DOI: 10.4169/math.mag.85.3.163.

[Rei03] Irving Reiner. *Maximal Orders*. London Mathematical Society Monographs new ser., 28. Oxford ; New York: Clarendon Press, 2003. 395 pp. URL: https://global.oup.com/academic/product/maximal-orders-9780198526735.

[Rib89] Kenneth A. Ribet. "Bimodules and Abelian Surfaces". In: *Algebraic Number Theory*. Vol. 17. Adv. Stud. Pure Math. Academic Press, Boston, MA, 1989, pp. 359–407. DOI: 10.2969/aspm/01710359.

[Rib90] Kenneth A. Ribet. "On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms". In: *Inventiones Mathematicae* 100.2 (1990), pp. 431–476. DOI: 10.1007/BF01231195.

[Roe23] David Roe. "Modular Curves in the LMFDB". Conference. Modular Curves and Galois Representations (Zagreb, Croatia). Sept. 21, 2023. URL: https://web.math.pmf.unizg.hr/~fnajman/Mod_curves.html.

[Roh97] David E. Rohrlich. "Modular Curves, Hecke Correspondence, and L-functions". In: *Modular Forms and Fermat's Last Theorem (Boston, MA, 1995)*. Springer, New York, 1997, pp. 41–100. DOI: 10.1007/978-1-4612-1974-3_3.

[Roq18] Peter Roquette. *The Riemann Hypothesis in Characteristic p in Historical Perspective*. Vol. 2222. Lecture Notes in Mathematics. Springer, Cham, 2018. ix+233. DOI: 10.1007/978-3-319-99067-5.

[Rov91] Josep Gonzalez Rovira. "Equations of Hyperelliptic Modular Curves". In: *Annales de l'Institut Fourier* 41.4 (1991), pp. 779–795. DOI: 10.5802/aif.1273.

[RS17] Kenneth A. Ribet and William A. Stein. "Lectures on Modular Forms and Hecke Operators". Book draft. 2017. URL: https://wstein.org/books/ribet-stein/.

[Sai13] Takeshi Saito. *Fermat's Last Theorem: Basic Tools*. Trans. by Masato Kuwata. Vol. 243. Translations of Mathematical Monographs. American Mathematical Society, Providence, RI, 2013. xiv+200. DOI: 10.1090/mmono/243.

[Sai14] Takeshi Saito. *Fermat's Last Theorem: The Proof*. Trans. by Masato Kuwata. Vol. 245. Translations of Mathematical Monographs. American Mathematical Society, Providence, RI, 2014. xvi+222. DOI: 10.1090/mmono/245.

[Sar90] Peter Sarnak. *Some Applications of Modular Forms*. Vol. 99. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 1990. x+111. DOI: 10.1017/CBO9780511895593.

[Sch08] René Schoof. "Four Primality Testing Algorithms". In: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*. Vol. 44. Math. Sci. Res. Inst. Publ. Cambridge Univ. Press, Cambridge, 2008, pp. 101–126. URL: https://www.math.leidenuniv.nl/~psh/ANTproc/05rene.pdf.

[Sch12] René Schoof. "On the modular curve $X_0(23)$". In: *Geometry and arithmetic*. EMS Ser. Congr. Rep. Eur. Math. Soc., Zürich, 2012, pp. 317–345. DOI: 10.4171/119-1/19.

[Sch82] René Schoof. “Quadratic Fields and Factorization”. In: *Computational Methods in Number Theory, Part II.* Vol. 155. Math. Centre Tracts. Math. Centrum, Amsterdam, 1982, pp. 235–286. URL: https://gkorpal.github.io/files/Schoof1982.pdf.

[Shi95] Mahoro Shimura. “Defining Equations of Modular Curves $X_0(N)$”. In: *Tokyo Journal of Mathematics* 18.2 (1995), pp. 443–456. DOI: 10.3836/tjm/1270043475.

[Shu09] Daniel Shumow. “Isogenies of Elliptic Curves: A Computational Approach”. MSc thesis. Seattle, United States: University of Washington, 2009. URL: http://arxiv.org/abs/0910.5370.

[Sie89] Carl Ludwig Siegel. *Lectures on the geometry of numbers.* Springer-Verlag, Berlin, 1989. x+160. DOI: 10.1007/978-3-662-08287-4. Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* 2nd ed. Vol. 106. Graduate Texts in Mathematics. New York, NY: Springer New York, 2009. DOI: 10.1007/978-0-387-09494-6. Errata and addenda http://www.math.brown.edu/johsilve/AECHome.html.

[Sil21] Javier Silva. “Zero-Knowledge Proofs and Isogeny-Based Cryptosystems”. PhD thesis. Barcelona, Spain: Universitat Pompeu Fabra, 2021. URL: https://hdl.handle.net/10803/671222.

[Sil93] Joseph H. Silverman. “Taxicabs and Sums of Two Cubes”. In: *American Mathematical Monthly* 100.4 (1993), pp. 331–340. DOI: 10.2307/2324954.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994. xiv+525. DOI: 10.1007/978-1-4612-0851-8. Errata and addenda http://www.math.brown.edu/johsilve/ATAECHome.html.

[Sma16] Nigel P. Smart. *Cryptography Made Simple.* Information Security and Cryptography. Cham: Springer International Publishing, 2016. DOI: 10.1007/978-3-319-21936-3.

[Sot20] Jana Sotáková. “Elliptic Curves, Isogenies, and Endomorphism Rings”. Lecture notes for ANTS-XIV Summer School. Auckland, New Zealand, 2020. URL: https://jana-sotakova.github.io/writings/ANTS_school_exposition.pdf.

[Sou16] Vladimir Soukharev. “Post-Quantum Elliptic Curve Cryptography”. PhD thesis. Waterloo, Canada: University of Waterloo, 2016. URL: http://hdl.handle.net/10012/10488.

[Sta21] Katherine E. Stange. *Frobenius and the endomorphism ring of $j = 1728$.* 2021. URL: https://math.colorado.edu/~kstange/papers/1728.pdf. preprint.

[Ste12] William A. Stein. “Algebraic Number Theory, a Computational Approach”. Book draft. 2012. URL: https://wstein.org/books/ant/.

[Sul13] Nick Sullivan. *A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography.* The Cloudflare Blog. Oct. 23, 2013. URL: https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/.

[Sut13] Andrew V. Sutherland. “Isogeny Volcanoes”. In: *ANTS X – Tenth Algorithmic Number Theory Symposium.* Vol. 1. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2013, pp. 507–530. DOI: 10.2140/obs.2013.1.507.

[Sut17] Andrew Sutherland. “Number Theory I”. Lecture notes for Math 18.785. MIT, 2017. URL: https://math.mit.edu/classes/18.785/2017fa/index.html.

[Sut22] Andrew Sutherland. “Elliptic Curves”. Lecture notes, problem sets, and Sage worksheets for Math 18.783. MIT, 2022. URL: https://math.mit.edu/classes/18.783/2022/index.html.

[SZ03] Susanne Schmitt and Horst G. Zimmer. *Elliptic Curves: A Computational Approach.* Vol. 31. De Gruyter Studies in Mathematics. Walter de Gruyter & Co., Berlin, 2003. x+367. DOI: 10.1515/9783110198010.

[Tat66] John Tate. “Endomorphisms of Abelian Varieties over Finite Fields”. In: *Inventiones mathematicae* 2.2 (1966), pp. 134–144. DOI: 10.1007/BF01404549.

[Tha22] Justin Thaler. *Proofs, Arguments, and Zero-Knowledge.* Vol. 4. Foundations and Trends in Privacy and Security. Norwell, MA: Now Publishers, 2022. DOI: 10.1561/3300000030. Current draft is available here https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.html.

[The23] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.0).* 2023. URL: https://www.sagemath.org.

[Tit79] J. Tits. “Reductive groups over local fields”. In: *Automorphic forms, representations and L-functions, Part 1*. Proc. Sympos. Pure Math., XXXIII. Amer. Math. Soc., Providence, R.I., 1979, pp. 29–69. DOI: `10.1090/pspum/033.1`. Scan of the paper: `https://gkorpal.github.io/files/Tits1979.pdf`.

[TVN07] Michael Tsfasman, Serge Vlăduţ, and Dmitry Nogin. *Algebraic Geometric Codes: Basic Notions*. Vol. 139. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2007. xx+338. DOI: `10.1090/surv/139`.

[TVN19] Michael Tsfasman, Serge Vlăduţ, and Dmitry Nogin. *Algebraic Geometry Codes: Advanced Chapters*. Vol. 238. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2019. x+453. DOI: `10.1090/surv/238`.

[Urb17] David Urbanik. *A Friendly Introduction to Supersingular Isogeny Diffie-Hellman*. 2017. URL: `https://www.math.toronto.edu/dburbani/work/friendlysidh.pdf`.

[vdLaa18] Harmke van der Laan. “Supersingular Isogeny Diffie-Hellman: Finding the Distribution of the Secret Key by Computation of Brandt Matrices”. BSc thesis. Groningen, Netherlands: University of Groningen, 2018. 38 pp. URL: `https://fse.studenttheses.ub.rug.nl/17892/`.

[Ven15] Daniele Venturi. “Zero-Knowledge Proofs and Applications”. Lecture notes. Tecniche di Sicurezza Informatica dei Dati e delle Reti, May 21, 2015. URL: `http://danieleventuri.altervista.org/files/zero-knowledge.pdf`.

[Ver23] Mattia Veroni. “A Study on Tighter and More Efficient Isogeny-Based Cryptographic Protocols”. PhD thesis. Trondheim, Norway: Norwegian University of Science and Technology, 2023. URL: `https://hdl.handle.net/11250/3060410`.

[vHoe97] Mark van Hoeij. “Rational Parametrizations of Algebraic Curves Using a Canonical Divisor”. In: *Journal of Symbolic Computation* 23.2-3 (Feb. 1997), pp. 209–227. DOI: `10.1006/jsco.1996.0084`.

[Voi05] John Voight. “Curves over Finite Fields with Many Points: An Introduction”. In: *Computational Aspects of Algebraic Curves*. Vol. 13. Lecture Notes Ser. Comput. World Sci. Publ., Hackensack, NJ, 2005, pp. 124–144. DOI: `10.1142/9789812701640_0010`.

[Voi13] John Voight. “Identifying the Matrix Ring: Algorithms for Quaternion Algebras and Quadratic Forms”. In: *Quadratic and Higher Degree Forms*. Developments in Mathematics. New York, NY: Springer, 2013, pp. 255–298. DOI: `10.1007/978-1-4614-7488-3_10`.

[Voi21] John Voight. *Quaternion Algebras*. Vol. 288. Graduate Texts in Mathematics. Cham: Springer International Publishing, 2021. DOI: `10.1007/978-3-030-56694-4`. Errata and addenda `http://quatalg.org`.

[Was08] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. 2nd ed. Discrete Mathematics and Its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2008. xviii+513. DOI: `10.1201/9781420071474`.

[Wat69] William C. Waterhouse. “Abelian Varieties over Finite Fields”. In: *Annales scientifiques de l’École normale supérieure* 2.4 (1969), pp. 521–560. DOI: `10.24033/asens.1183`.

[Wei13] Jared Weinstein. “Modular Curves at Infinite Level”. Lecture notes for AWS - Modular forms and modular curves. Tucson, 2013. URL: `https://swc-math.github.io/aws/2013/2013WeinsteinLectureNotes.pdf`.

[Wes01] Tom Weston. *The modular curves $X_0(11)$ and $X_1(11)$*. 2001. URL: `https://swc-math.github.io/aws/2001/01Weston1.pdf`. preprint.

[Wes22] Benjamin Wesolowski. “The Supersingular Isogeny Path and Endomorphism Ring Problems Are Equivalent”. In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. Denver, CO, USA: IEEE, 2022, pp. 1100–1111. DOI: `10.1109/FOCS52979.2021.00109`.

[Yu09] Jiu-Kang Yu. “Bruhat-Tits theory and buildings”. In: *Ottawa lectures on admissible representations of reductive p-adic groups*. Vol. 26. Fields Inst. Monogr. Amer. Math. Soc., Providence, RI, 2009, pp. 53–77. DOI: `10.1090/fim/026/02`. Scan of the paper: `https://gkorpal.github.io/files/Yu2009.pdf`.

"If you ever think while writing a thesis, phd, master’s, or bachelor’s, that ‘no one will ever read this’, know that I will. I will read it."
- Deirdre Connolly (Aug 08, 2022), https://twitter.com/durumcrustulum/status/1556716005337944064