Isogenies of elliptic curves defined over $\mathbb{F}_p$, $\mathbb{Q}$, and their extensions

Joanna Gaski

December 10, 2010

1 Introduction

This paper introduces the maps between elliptic curves known as isogenies, providing definitions and basic background information about how these maps work over the standard fields $\mathbb{F}_p$, $\mathbb{Q}$, and their extensions. This will include the relationship between the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E and the isogenies defined to and from E, as well as the central role of the Frobenius endomorphism over a field of prime characteristic.

We will then look at the properties of an elliptic curve which are preserved by isogeny, and discuss general methods to determine if two curves are isogenous, and to explicitly calculate an isogeny of elliptic curves.

The last part of the paper will present results about the isogenies which occur among curves defined over $\mathbb{Q}$ and extension fields. These will include theoretical results about the possible prime degrees of an rational isogeny between $\mathbb{Q}$-curves (Mazur), as well as explicit examples and data about isogeny degrees and equivalence classes occurring over $\mathbb{Q}$ (Cremona) and certain real quadratic number fields (Elkies).

2 Why study isogenies?

Research in the area of isogenies among elliptic curves is rich and complex, as is the mathematics underlying these relationships. An isogeny is a nonconstant morphism between elliptic curves, which among other interesting properties, respects the underlying additive group operation of each curve. These maps between curves are of interest both for their mathematical properties and for their applications in elliptic curve cryptography (ECC).

2.1 What we would like to know

If E_1 and E_2 are two isogenous elliptic curves defined over a field K, then information about the structure of one curve will reveal information about the other. Isogeny among elliptic curves forms an equivalence relation. Exact statements of the properties of an elliptic curve E_1 which are preserved by isogeny vary based on the field K of definition, and we will try to illuminate some of these relationships. Indeed, even what isogenies can occur at all between elliptic curves over a field K depends on K itself, and so we can understand the structure of K more deeply by studying its isogeny classes.

Among the questions of interest are:

- Given elliptic curves E_1 and E_2 defined over a field K, how do we determine whether E_1 and E_2 are isogenous, and what (if any) degree of isogeny exists between them?
- In the case that two curves are isogenous, how do we find an explicit map between them?
- What aspects of the structure of E_1 and E_2 determine (or limit) possible isogenies? Are they isogenous over some extension field of K?
- Given a single curve E, how do we find any other curves with which it is isogenous? What is the structure of the isogeny class of E (to be defined later)?
- Given a field K, what are the possible degrees of any isogeny between curves defined over that field, what examples have been explicitly found (if the question is unresolved), and what theoretical results limit those possible degrees?
- What proportion of curves over K admit a non-trivial isogeny?
- What questions remain open?

2.2 Elliptic Curve Cryptography

The area of elliptic curve cryptography is closely tied to the general topic of isogenies because so much isogeny research has been done in the context of cryptography. Isogenies have both been used as key tools in ECC algorithms, as well as been the focus of extensive study themselves, and the distinction between ECC research and other elliptic curve research is not always clear. This is a short list of some of the research where isogenies have played a key role, and which has advanced the theory of

isogenies, but the list could go on. We will revisit only some of this research in later sections, but it is all interesting, and gives an idea of the use of isogenies in practice.

From the early 1990's, isogenies have been used as a tool in point counting algorithms for elliptic curves over finite fields. The Elkies & Atkin (SEA) improvements to René Schoof's original 1985 algorithm for point counting made use of isogenies and the modular polynomials, resulting in an algorithm which can be used for curves over finite fields of order several hundred digits [9]. Couveignes and Morain extended SEA ideas to prime powers, composing isogenies to compute a factor of the l^k-th division polynomial when the Frobenius endomorphism has two distinct rational eigenvalues. Lercier later developed an algorithm for computing l-isogenies (as in SEA) when $p \ll l$.

David Kohel's 1996 PhD thesis involved algorithms for determining the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve over a finite field, and the graph of l-isogenies of a supersingular curve $E/\mathbb{F}_{p^2}$ [6]. His work used the ideas of an elliptic curve lying at the surface, at the floor of rationality, or at a certain depth to describe the action of isogenies and the field of definition of E. Fouquet and Morain extended Couveignes & Morain's work to the case where the Frobenius has only one eigenvalue, in the context of Kohel's endomorphism ring work, including other general results on isogenies [5]. Bröker & Stevenhagen gave an algorithm to construct an elliptic curve E and finite field K such that $|E/K|$ has a given prime order, using CM (an isogeny relation we will look at later).

Also recently, isogenies between elliptic curves are being used as tools in the MOV attack for the discrete logarithm problem (DLP), for complexity analysis in reducing the DLP, and to analyze parameter selection for cryptosystems. They have uses in provably secure random number generation and hash functions as well. With their widespread utility in cryptographic applications as well as more general number theoretic and algebraic interest, isogenies have become a valuable tool for working with elliptic curves which is worth thoroughly understanding.

3 Basic structure of isogenies

We begin with the definitions of an isogeny and its degree, and a look at the fundamental properties of this type of map. An elliptic curve E over a field K is a complete curve of genus one, given by a Weierstrass equation with coefficients in K

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a6$$

and having a unique point O at infinity. The points $P = (x, y) \in E_{/K}$ admit an abelian group structure, with O as the identity, whose additive operation is given by a well known geometric group law taking E x $E \to E$, which is a morphism of varieties. Explicit rational functions for the group law are given by Silverman [11, III.2].

Definition 1 (Isogeny of elliptic curves)**.** *Let E_1 and E_2 be two elliptic curves defined over a field K. An* isogeny φ *from E_1 to E_2 is a nonconstant morphism of curves*

$$\varphi : E_1 \longrightarrow E_2$$

which maps O_{E_1}, the unique point at infinity of E_1, to O_{E_2}.

We disallow the trivial map $\varphi = \mathsf{O}$, and say that two curves are isogenous over K if there is an isogeny of E_1 to E_2 defined over K. Note that an isogeny is not necessarily an isomorphism because an isogeny may have a non-trivial kernel. Also note that an isomorphism is not necessarily an isogeny, because an isomorphism may not map O to O. For example, the translation by Q map, $\tau_Q : E \to E$ given by $\tau_Q : P \mapsto P + Q$ where $Q \in E$, is clearly an isomorphism, but is only an isogeny if $Q = \mathsf{O}$.

As a morphism of smooth curves, an isogeny φ is either constant or surjective, and since we have disallowed the zero map, we therefore have a surjection of algebraic varieties [11].

Theorem 1 (Homomorphism of groups [11, III 4.8])**.** *Let $\varphi : E_1 \longrightarrow E_2$ be an isogeny. Then*

$$\varphi(P + Q) = \varphi(P) + \varphi(Q) \text{ for all } P, Q \in E_1.$$

Hence the map φ preserves the group structure of E_1, and is a homomorphism of groups. We denote the collection of homomorphisms over K from E_1 to E_2 as $\mathrm{Hom}_K(E_1, E_2)$, and let $\mathrm{End}_K(E) = \mathrm{Hom}_K(E, E)$. When referring to morphisms over $\bar{K}$, we write $\mathrm{Hom}(E_1, E_2) = \mathrm{Hom}_{\bar{K}}(E_1, E_2)$ and $\mathcal{O} = \mathrm{End}(E) = \mathrm{End}_{\bar{K}}(E)$.

The isogeny $\varphi : E_1 \to E_2$ induces an injection of function fields fixing K [11, III.4]:

$$\varphi^* : \bar{K}(E_2) \hookrightarrow \bar{K}(E_1)$$

$$\varphi^* : f \longmapsto f \circ \varphi.$$

There is another way to define an isogeny, from a computational viewpoint.

Definition 2 (Isogeny of Elliptic Curves [13, 8.6])**.** *For elliptic curves E_1 and E_2 over K, an isogeny is a homomorphism from $E_1(\bar{K})$ to $E_2(\bar{K})$ that is given by rational functions:*

$$\varphi : E_1(\bar{K}) \longrightarrow E_2(\bar{K})$$
$$\varphi : (x, y) \longmapsto (\frac{p_x}{q_x}, \frac{p_y}{q_y}).$$

Definition 3 (Degree of an isogeny)**.** *Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves. Then the* degree *of φ is the degree of the field extension $\bar{K}(E_1)/\varphi^*\bar{K}(E_2)$. We say that φ is separable, inseparable, or purely inseparable according to this field extension.*

Definition 4 (Degree of an isogeny)**.** *Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves, with $\varphi : (x, y) \mapsto (\frac{p_x}{q_x}, \frac{p_y}{q_y})$. Then the* degree *of φ is the maximum of the degrees of the polynomials p_x and q_x.*

Definition 5 (Separable degree of an isogeny)**.** *Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves. Then the* separable degree *$deg_s(\varphi)$ of φ is the cardinality of the kernal $\ker \varphi = \varphi^{-1}(\mathsf{O})$ of the map.*

A field extension L of K is always separable in the case that K has characteristic zero, so the only time that we can have an inseparable isogeny φ is when we have defined E over a field of characteristic $p \neq 0$. In this case, φ can be decomposed into two isogenies, one separable and one purely inseparable (details in section on fields of prime characteristic). More generally, if the degree of an isogeny is composite, it can be decomposed into a composition of isogenies of prime degree.

Example 1 (Multiplication by m map)**.** *Let E be the elliptic curve given by $y^2 = x^3 + Ax + B$, and let ψ_i be the division polynomials given by*

$$\begin{aligned}
&\psi_1 = 1,\\
&\psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,\\
&\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, && \text{for } m \geq 2,\\
&\psi_{2m} = \left(\frac{\psi_m}{2y}\right) \cdot \left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right), && \text{for } m \geq 3.
\end{aligned}$$

Then for $P = (x, y) \in E$, the multiplication by $m \neq 0$ map *is a self-isogeny given by*

$$[m] : E \longrightarrow E,$$

$$[m] : P \longmapsto P + P + \cdots P,$$

or expressed in rational functions:

$$[m]P = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{2m}}{2\psi_m^4} \right).$$

Here, $\ker \varphi = E[m]$ is the set of m-torsion points of E, and $[m]$ is separable with degree m^2. In the case that char $K = 0$ or $\gcd(m, \text{ char } K) = 1$, then

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \text{ x } \mathbb{Z}/m\mathbb{Z}.$$

Otherwise [11, III 6.4], char $K = p|m$, and for all $r \in \mathbb{Z}_{>0}$, one of the following occurs:

$$E[p^r] = \mathsf{O}, \text{ or} \tag{1}$$
$$E[p^r] = \mathbb{Z}/p^r\mathbb{Z}. \tag{2}$$

In the first case, E is said to be supersingular, and in the second case, it is said to be ordinary.

4 The dual isogeny

Theorem 2 (Dual isogeny)**.** *Let E_1 and E_2 be two elliptic curves defined over a field K, and let $\varphi : E_1 \to E_2$ be an isogeny of degree l. Then there is a unique isogeny $\hat{\varphi} : E_1 \to E_2$, called the dual isogeny, such that*

1. *$\hat{\varphi} : E' \to E$ is an isogeny of degree l,*
2. *$\hat{\varphi} \circ \varphi$ is the multiplication by l map on E.*
3. *$\varphi \circ \hat{\varphi}$ is the multiplication by l map on E'.*

For additional properties of the dual isogeny and proof, see Silverman [11, III 6]. The existence of the dual isogeny causes the isogeny relationship to be an equivalence relation of elliptic curves, so that we may speak of the isogeny class of an elliptic curve. The isogeny class of en elliptic curve is a set of pairwise non-isomorphic elliptic curves, well-defined up to isomorphism.

A theorem of Shafarevitch implies that for an elliptic curve E/K, the equivalence class of curves E'/K that are K-isogenous to E is finite [11, IX 6.2].

Example 2 (Dual isogeny)**.** *Let E be given by $y^2 = x^3 + Ax^2 + Bx$, and E' be given by $y'^2 = x'^3 - 2Ax'^2 + (A^2 - 4B)x'$. Then the maps given by*

$$\varphi : (x, y) \longmapsto \left(\frac{y^2}{x^2}, \frac{y(x^2 - B)}{x^2} \right) = (x', y'), \qquad \varphi(0,0) = \varphi(\mathsf{O}) = \mathsf{O}$$

$$\varphi' : (x', y') \longmapsto \left(\frac{y'^2}{4x'^2}, \frac{y'(x'^2 - A^2 + 4B)}{8x'^2} \right) = (x, y), \qquad \varphi'(0,0) = \varphi'(\mathsf{O}) = \mathsf{O}$$

are each a degree 2 isogeny, with kernel equal to $\{(0,0), \mathsf{O}\}$ of the respective curves. The composition $\varphi' \circ \varphi$ is the $[2]E$ multiplication by 2 map on E [13, p. 236].

5 The Frobenius isogeny

Example 3 (Frobenius endomorphism)**.** *If $K = \mathbb{F}_q$ is a finite field of q elements, then the Frobenius emdomorphism ϕ on $\bar{K}$, given by $\phi : x \mapsto x^q$, generates $Gal(\bar{K}/K)$ and fixes K. If we let E be an elliptic curve defined over K, and define $\pi(\mathsf{O}) = \mathsf{O}$, then the Frobenius endomorphism determines an isogeny:*

$$\pi : E \longrightarrow E$$

$$\pi : (x, y) \longmapsto (x^q, y^q)$$

$$\pi : \mathsf{O} \longmapsto \mathsf{O}.$$

The Frobenius endomorphism satisfies its characteristic polynomial,

$$x^2 - a_q x + q = 0,$$

where a_q is the trace of Frobenius. A theorem of Tate states that the characteristic polynomial of π determines the isogeny class of E. The relationship is $|E(\mathbb{F}_q)| = q + 1 - a_q$, and the computation of a_q has been the focus of extensive ECC research.

The Frobenius isogeny is purely inseparable and has degree q. Furthermore, if $\varphi : E_1 \to E_2$ is any isogeny between smooth curves defined over K where K has characteristic p, then φ can be decomposed into a composition of morphisms, one of which is separable, and one of which is the purely inseparable Frobenius isogeny π. The composition is $\varphi = \psi \circ \pi$:

$$E_1 \xrightarrow{\pi} E_1^{(q)} \xrightarrow{\psi} E_2$$

where $\deg \psi = [\deg \varphi]_s$, and $\deg \pi = [\deg \varphi]_i = q = p^r$ for some integer $r \geq 1$ [11, II.2.12].

6 The endomorphism ring of E

Since the multiplication by m map is defined over K and takes $E \to E$ and $\mathsf{O} \mapsto \mathsf{O}$, it is an endomorphism in $\mathrm{End}_K(E) \subset \mathrm{End}(E)$. The set $\mathcal{O} = \mathrm{End}(E)$ of endomorphisms of E has a natural group structure based on the group structure of E. With composition of morphisms as a second operation, $\mathcal{O}$ has a natural ring structure. So the $[m]$ map allows us to define an injection of rings

$$[\,] : \mathbb{Z} \hookrightarrow \mathrm{End}(E).$$

In general, $\mathrm{Hom}(E_1, E_2)$ is a torsion free $\mathbb{Z}$ module of rank at most 4, while $\mathrm{End}(E)$ in particular is an integral domain of characteristic zero [11, III 4.2,III 7.5]. So $\mathrm{End}(E) \geq \mathbb{Z}$, and when the inclusion is strict, we say that the curve E has complex multiplication (CM). The possibilities for the isomorphism type of $\mathrm{End}(E)$ are $\mathbb{Z}$, an order in a quadratic imaginary extension of $\mathbb{Q}$, or an order in a definite quaternion algebra over $\mathbb{Q}$.

When K has characteristic p, $\mathrm{End}(E)$ is always strictly greater than $\mathbb{Z}$, and is generated by the p-power Frobenius endomorphism, which we will look at in the section on fields of non-zero characteristic. Specifically, when E is an ordinary elliptic curve (2), $\mathrm{End}(E)$ is isomorphic to an imaginary quadratic order. When E is supersingular (1), $\mathrm{End}(E)$ is isomorphic to an order in a quaternion algebra [11, V.3].

When E is defined over a field of characteristic zero, $\mathrm{End}(E)$ has isomorphism type either $\mathbb{Z}$ or an order of an imaginary quadratic field [11, III 9.4]. In the second case, E is said to have complex multiplication (CM).

Example 4 (Complex multiplication)**.** *Let E/K be the elliptic curve defined by the equation*

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

where $char(K) = 0$. Then if $i \in \bar{K}$ is a primitive fourth root of unity, there is an endomorphism of E given by

$$[i] : (x, y) \mapsto (-x, iy).$$

This map satisfies

$$[i] \circ [i] : (x, y) \mapsto (x, -y) = -(x, y),$$

and induces a ring homomorphism

$$\phi : \mathbb{Z}[i] \to \ End(E)$$

$$\phi : a + bi \mapsto [a] + [b] \circ [i].$$

In this case, $End(E) \simeq \mathbb{Z}[i]$.

7 Isogeny invariants

7.1 Point count over a finite field

Over a finite field, there is a very clear criterion for whether two curves are isogenous. This is one of the reasons that elliptic curve isogenies can be used in cryptographic attacks: an isogenous curve over $\mathbb{F}_q$ will have the same number of points as the original curve.

Theorem 3 (Tate)**.** *Let E_1 and E_2 be two elliptic curves defined over a finite field $\mathbb{F}_q$. Then E and E' are isogenous if and only if $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$.*

Additionally, for a isogenous pair of curves defined over $\mathbb{Q}$ or an extension field, this point count property will descend to point counts over the (finite) residue fields of each curve.

7.2 Reduction characteristics and conductor

Let K be a field of characteristic zero. We say that a curve E/K has good (or stable) reduction at a prime $\mathfrak{p} \in O_K$, the ring of integers of K, if the curve $E/K_\mathfrak{p}$ is non-singular, where $K_\mathfrak{p}$ is the residue field of O_K at $\mathfrak{p}$. Similary, E/K has multiplicative (bad, semistable) reduction at $\mathfrak{p}$ if $E/K_\mathfrak{p}$ has a node, and additive (bad, unstable) reduction at $\mathfrak{p}$ if $E/K_\mathfrak{p}$ has a cusp. By $E/K_\mathfrak{p}$ we mean the Weierstrass equation of E/K reduced modulo $\mathfrak{p}$, which may not define an elliptic curve.

The reduction characteristics of E/K are encoded in the curve's conductor $N_{E/K}$, which is an ideal in O_K defined by

$$N_{E/K} = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{f(E/K_\mathfrak{p})}$$

where

$$f(E/K_\mathfrak{p}) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } \mathfrak{p} \\ 1 & \text{if } E \text{ has multiplicative reduction at } \mathfrak{p} \\ 2 + \delta_\mathfrak{p} & \text{if } E \text{ has additive reduction at } \mathfrak{p}. \end{cases}$$

Here, $\delta_\mathfrak{p} = 0$ when the characteristic of the residue field $K_\mathfrak{p}$ is greater than or equal to 5. When the characteristic of $K_\mathfrak{p}$ is 2 or 3, $\delta_\mathfrak{p}$ is an integer which depends on the action of the inertia group at $\mathfrak{p}$ of $\mathrm{Gal}(\bar{K}/K)$ on the torsion subgroup of E. Details are in Silverman [12, IV.10]. Both reduction properties and the conductor of an elliptic curve are defined in Silverman for E over a local field K, but when dealing

with a number field, we can instead consider the reduction of E over the local field $K_\mathfrak{p}$.

The conductor of E/K is preserved by isogeny [12, IV.11 ex 4.40], and so comparison of the conductors of two elliptic curves over a number field K can be used to rule out the possibility of an isogeny between them, in the case of inequality of conductors.

7.3 Residue field point counts and Falting's theorem

If E_1 and E_2 are isogenous over K, then for any prime $\mathfrak{p} \in O_K$, E_1 will have good reduction at $\mathfrak{p}$ if and only if E_2 does. And in the case of good reduction at $\mathfrak{p}$, we will have the equality $|E_1/K_\mathfrak{p}| = |E_2/K_\mathfrak{p}|$. Faltings proved that the converse holds. If E_1/K and E_2/K are elliptic curves over a number field K, and S is the set of primes of O_K at which E_1 and E_2 have good reduction, then

$$|E_1/K_\mathfrak{p}| = |E_2/K_\mathfrak{p}| \text{ for all } \mathfrak{p} \in S \Rightarrow E_1/K \text{ and } E_2/K \text{ are isogenous.}$$

Hence, any differing point count $|E_1/K_\mathfrak{p}| \neq |E_2/K_\mathfrak{p}|$ is sufficient to prove that E_1 and E_2 are not isogenous.

8 General results

8.1 Vélu's explicit computation of an isogeny and resulting curve

Because the kernel of an isogeny from E/K is a finite subgroup of E, we have the following.

Proposition 1. *[11, III 4.12] Let E be an elliptic curve, and let Φ be a finite subgroup of E. There there are a unique elliptic curve E' and a separable isogeny φ satisfying*

$$\varphi : E \to E' \text{ and } \ker \varphi = \Phi.$$

Furthermore, if the subgroup Φ is invariant under the action of $\mathrm{Gal}(\bar{K}/K)$, then both the isogeny φ and the curve E' can be defined over K. The isogenous curve is often referred to simply as E/Φ.

A formula of Vélu computes the codomain E/Φ and isogeny φ in the following manner. If E is given by the general Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a6,$$

then for a point $Q = (x_Q, y_Q) \in \Phi$ with $Q \neq \mathsf{O}$, we define

$$\begin{aligned} g_Q^x &= 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q \\ g_Q^y &= -2y_Q - a_1x_Q - a3 \\ v_Q &= \begin{cases} g_Q^x & (\text{if } 2Q = \mathsf{O}) \\ 2g_Q^x & (\text{if } 2Q \neq \mathsf{O}) \end{cases} \\ u_Q &= (g_Q^y)^2. \end{aligned}$$

We then choose a subset $S \subset \Phi$ containing all order 2 points, and one of each pair of order ≥ 3 points, and compute

$$v = \sum_{Q \in S} v_Q, \qquad\qquad w = \sum_{Q \in S} (u_Q + x_Q v_Q).$$

Then an isogenous curve E' will be given by the Weierstrass equation

$$y'^2 + A_1x'y' + A_3y' = x'^3 + A_2x'^2 + A_4x + A6,$$

where

$$A_1 = a_1,\ A_2 = a_2,\ A_3 = a_3,$$
$$A_4 = a_4 - 5v,\ A_6 = a_6 - (a_1^2 + 4a_2)v - 7w.$$

Further details and a proof of correctness are in Washington [13, 12.3], and there have been extensive implementations of algorithms to compute an isogeny based on Vélu's formulae.

9 Results over $\mathbb{Q}$, algebraic extensions, and $\mathbb{C}$

9.1 Torsion points

When looking at isogenies over a field K of characteristic zero, any degree d isogeny will correspond to an order d subgroup of $E(\bar{K})$. So we begin by looking at what is known of the order of any possible finite subgroups of $E(K)$ or $E(\bar{K})$.

Theorem 4 (Mordell-Weil)**.** *If K is a number field and E/K is an elliptic curve, then the group $E(K)$ is a finitely generated [11, VIII 6.7]. abelian group.*

So, when K is any finite algebraic extension of $\mathbb{Q}$, there is a set of points P_1, P_2, …, P_n in $E(K)$ such that if Q is any point in $E(K)$, then Q can be expressed as a linear combination $Q = a_1P_1 + a_2P_2 + \ldots + a_nP_n$.

It follows then from the general theory of the structure of finitely generated abelian groups that the set of K-rational points on E, known as $E(K)$ and called the Mordell-Weil group, can be decomposed into a torsion group and a non-torsion group, so that

$$E(K) \simeq E(K)_{torsion} \oplus \mathbb{Z}^{R_E}$$

where R_E is the analytic rank of $E(K)$.

When $K = \mathbb{Q}$, a conjecture of Ogg which was later proved by Mazur [8], states that for any elliptic curve E defined over $\mathbb{Q}$, the torsion group of $E(\mathbb{Q})$ is one of the following fifteen groups:

$\mathbb{Z}/m\mathbb{Z}$	for $1 \leq m \leq 10$, or $m = 12$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$	for $1 \leq m \leq 4$.

When K is an algebraic extension of $\mathbb{Q}$ of degree $[K : \mathbb{Q}] \leq d$ $(d \geq 1)$, Merel later proved that there is a constant $N(d)$, such that for any elliptic curve E defined over K, $|E_{tors}(K)| \leq N(d)$.

For torsion points of $E(\mathbb{C})$, we know that $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$, meaning that E has $m + 1$ order m subgroups which reside in $\mathbb{C}^2$. This would imply that

$$E(\mathbb{C})_{tors} \simeq (\mathbb{Z}/p_1\mathbb{Z})^{\oplus 2} \oplus (\mathbb{Z}/p_2\mathbb{Z})^{\oplus 2} \oplus \dots$$

for all primes $p_i \in \mathbb{Z}$.

However, for an arbitrary elliptic curve E defined over $\bar{\mathbb{Q}}$, E must also be defined over the number field $K = \mathbb{Q}(a_1, a_2, a_3, a_4, a_6)$, where the a_i are the Weierstrass coefficients of E, and therefore Merel's $|E_{tors}(K)| \leq N(d)$ upper bound would apply.

9.2 Over $\mathbb{Q}$

In *Rational isogenies of prime degree*, Barry Mazur analyzed results about several previously studied $\mathbb{Q}$-rational N-isogenies among elliptic curves over $\mathbb{Q}$, and provided a landmark proof excluding isogenies of any other degree over $\mathbb{Q}$. The following is a brief presentation of some of the results from that paper, and a reproduction of the table of isogenies over $\mathbb{Q}$, with a summary of their source [8].

For these results, $\Gamma_0(N)$ is the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_0(N) = \left\{ \alpha \in \mathrm{SL}_2(\mathbb{Z}) \colon \alpha \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \bmod N. \right\}$$

Let $\mathbb{H}$ denote the complex upper half plane. In general, a point $\tau \in \mathbb{H}$ corresponds to an isomorphism class of elliptic curves defined over $\mathbb{C}$ via a bijection ϕ between $\mathbb{C}/\Lambda_\tau$ and $E(\mathbb{C})$ where $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ is a lattice in $\mathbb{C}$, and ϕ is given by

$$\phi : \mathbb{C}/\Lambda_\tau \longrightarrow E_{\Lambda_\tau}(\mathbb{C})$$

$$\phi : z \longmapsto (\wp(z;\Lambda_\tau), \wp'(z;\Lambda_\tau)),$$

where $\wp$ is the Weierstrass $\wp$ function

$$\wp(z) = \wp(z;\Lambda_\tau) = \frac{1}{z^2} + \sum_{\omega \in \Lambda_\tau \setminus \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

The correspondence is described fully in Silverman [11, VI 2-6]. A point τ in the moduli space $\mathbb{H}/\Gamma_0(N)$ corresponds to an equivalence class of pairs (E, C) where E is an elliptic curve defined over $\mathbb{C}$ and $C \subset E(\mathbb{C})$ is a cyclic subgroup of order N. Specifically, there is a smooth projective curve $X_0(N)(\mathbb{Q})$ and a complex analytic isomorphism

$$j_{N,0} : \mathbb{H}^*/\Gamma_0(N) \longrightarrow X_0(N)(\mathbb{C})$$

where each equivalence class will have a pair (E, C) with E defined over $K = \mathbb{Q}(j_{N,0}(\tau))$ and C rational over K [11, C.13.1].

Theorem 5 (Mazur)**.** *Let N be a prime number such that the genus of $X_0(N)$ is > 0 (i.e. $N = 11$, or $N \geq 17$). Then there are no elliptic curves over $\mathbb{Q}$ possessing $\mathbb{Q}$-rational N-isogenies except when $N =$ 11, 17, 19, 37, 43, 67, or 163. Equivalently, there are no noncuspidal $\mathbb{Q}$-rational points on $X_0(N)$ except for the above values of N. In these cases, a complete list of the $\mathbb{Q}$-rational noncuspidal points of $X_0(N)$ is given by the table.*

N	g	v	N	g	v	N	g	v
≤ 10	0	∞	11	1	3	27	1	1
12	0	∞	14	1	2	37	2	2
13	0	∞	15	1	4	43	3	1
16	0	∞	17	1	2	67	5	1
18	0	∞	19	1	1	163	13	1
25	0	∞	21	1	4			

In this table, g is the genus of $X_0(N)$, and v is the number of non-cuspidal points of $X_0(N)$, which corresponds to the number of rational N-isogenies.

Let us note how surprising this result is. For any of the N-isogenies above where N is prime, the kernel is a subgroup of $E(\bar{\mathbb{Q}})$ of order N. We know that any elliptic curve defined over $\mathbb{Q}$ (or over $\mathbb{C}$, $\bar{\mathbb{Q}}$, or a number field for that matter) has an N-torsion subgroup $E[N]$ whose coordinates lie in $\mathbb{C} \cup \{\mathsf{O}\}$, $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ for every integer $N > 1$. We also know that any order p subgroup of $E(\mathbb{C})$ gives rise to a degree p isogeny from E to another elliptic curve over $\mathbb{C}$. So the question is, why are so few of these isogenies $\mathbb{Q}$-rational, and between $\mathbb{Q}$-curves?

In the case of $\mathbb{Q}$, Baker, Heegner, and Stark have shown that the non-composite numbers N for which the class number of $\mathbb{Q}(\sqrt{-N})$ is one are $\{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Recall that when E is defined over a number field K and has complex multiplication, that $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic field L. The case when L has class number one corresponds to the case when there is a curve E' isomorphic to E, with $\mathrm{End}(E')$ equal to the full ring of integers in L and E' defined over $\mathbb{Q}$ [11, C.11].

Another result from Mazur and Kenku addresses the question of how many mutually non-isomorphic elliptic curves can be isogenous to one another. An earlier theorem of Manin had proven that for any prime p, there is a constant C_p such that any elliptic curve E over $\mathbb{Q}$ is $\mathbb{Q}$-isogenous to at most C_p other $\mathbb{Q}$-curves by a p-power isogeny. By limiting the possible prime degrees of $\mathbb{Q}$-isogenies over $\mathbb{Q}$, to those in $S = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$, Mazur was able to give the bound $C = \prod_{p \in S} C_p$ for the size of the isogeny class of a $\mathbb{Q}$-curve. Further work limited the maximum isogeny class over $\mathbb{Q}$ to exactly eight mutually non-isomorphic $\mathbb{Q}$-curves.

John Cremona has also produced a database of elliptic curves over $\mathbb{Q}$ of conductor up to $130,000$, which is available online, with some extremely interesting analysis. The following is a reproduction of one table of his from a talk which he gave at the 7th Algorithmic Number Theory Symposium in 2006 about this database [3].

D	Size	# classes	%
1	1	372191	65.43
2	2	123275	21.67
3	2	31372	5.52
4	4	27767	4.88
5	2	2925	0.51
6	4	3875	0.68
7	2	808	0.14
8	6	2388	0.42
9	3	2709	0.48
10	4	271	0.05
11	2	60	0.01
12	8	286	0.05
13	2	130	0.02

D	Size	# classes	%
14	4	28	< 0.01
15	4	58	0.01
16	8	270	0.05
17	2	8	< 0.01
18	6	162	0.03
19	2	12	< 0.01
21	4	30	0.01
25	3	134	0.02
27	4	33	0.01
37	2	20	< 0.01
43	2	7	< 0.01
67	2	4	< 0.01
163	2	1	< 0.01

Here, D is the degree of isogeny and size is the number of curves in the isogeny class. We can observe the larger proportion of isogeny degrees corresponding to the possible torsion group orders of $E(\mathbb{Q})$, and also that the maximal size of an isogeny class, eight, is realized. However, I don't know of a result or conjecture predicting the frequency of occurrence of isogeny class size or of isogenies of each degree.

9.3 Over a quadratic extension $\mathbb{Q}(\sqrt{d})$

9.3.1 Quadratic imaginary fields

Mazur's 1978 paper [8] also proved several facts about isogenies over an imaginary quadratic extension K of $\mathbb{Q}$, reduction of an elliptic curve over K, and possible torsion points of $E(K)$.

Theorem 6 (Mazur)**.** *Let K be a quadratic imaginary field. There is a finite set of (rational) prime numbers $\mathcal{N}(K)$ such that if N is a rational prime which remains prime in K and $N \notin \mathcal{N}(K)$, then there are no K-rational N-isogenies of elliptic curves over K.*

So the set of possible prime degrees p of an isogeny over K, where p is inert in K, was proven finite, but the set of primes $\mathcal{N}(K)$ was not effectively determined in that paper.

For primes N which split in K, an earlier Mazur result states that there are quadratic imaginary fields K possessing K-rational N-isogenies for infinitely many primes. However, for all but finitely many of these primes, the N-isogenies are obtained by complex multiplication.

9.3.2 Real quadratic fields

I do not know of other theoretical results limiting the set of primes p for which there can be a K-rational p isogeny over K when K is a real quadratic number field.

Noam Elkies has a table of 621 elliptic curves defined over real quadratic extensions $\mathbb{Q}(\sqrt{D})$ [4] with discriminant $D < 10^6$ and j-invariant not in $\mathbb{Q}$, meaning that they are not defined over $\mathbb{Q}$, all of which have unit conductor. His observations of elliptic curve isogenies among this set are interesting. Some isogenies (as listed) are among non $\mathbb{Q}$-curves, and not all are of degree seen for elliptic curves over $\mathbb{Q}$.

The table includes nontrivial N-isogenies of degree

N	D, $\mathbb{Q}$-curves	not involving $\mathbb{Q}$-curves
2	337, 881, 2657, 6817, 14897, 28817, 50881, 130577	4092, 93193
3	109, 997	733, 18541, 193189
5	349, 461, 509, 1709	509
2	24, two CM curves	
28	28, two CM curves, isog to $\mathbb{Q}$-curves	
3	33, two CM curves, isog to $\mathbb{Q}$-curves	
15	29, two isogenous non-CM conjugate pairs	
8	41, two isogenous non-CM conjugate pairs	
4	65, six non-CM isogenous curves.	

Inerestingly, there are curves with a degree 28 isogeny between them, which does not happen over $\mathbb{Q}$ [2, p. 98].

9.4 Over a number field K

Mazur's 1978 results over imaginary quadratic fields do not extend to general number fields.

References

[1] Ian Blake, Gadiel Seroussi & Nigel Smart, *Elliptic curves in cryptograhy*, volume 265 of London Mathematical Society Lecture Note Series, Cambridge University Press, (2002)

[2] John Cremona, *Algorithms for modular elliptic curves*. 2nd edition, Cambridge University Press, (1997).

[3] John Cremona, *The elliptic curve database*, proceeding of the 7th international symposium ANTS VII, online at http://www.math.tu-berlin.de/~kant/ants/Proceedings/cremona/cremona_talk.pdf, (2006).

[4] Noam Elkies, *Elliptic curves of unit discriminant over real quadratic number fields*, online at http://math.harvard.edu/ elkies/rqfu/.

[5] M. Fouquet & F. Morain, *Isogeny volcanoes and the SEA algorithm*, ANTS-V, vol 2369 of LNCS, (2000).

[6] David Kohel, *Endomorphism rings of elliptic curves over finite fields*, Doctoral Thesis, Department of Mathematics, University of California at Berkeley, (1996).

[7] R. Lercier and F. Morain, *Algorithms for computing isogenies between elliptic curves*, AMS/IP Studies in Advanced Mathematics, Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin, volume **7**, 77-96, (1998).

[8] Barry Mazur, *Rational isogenies of prime degree*, Inventiones mathematicae, **44**, 129-162, (1978).

[9] René Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie de Nombres de Bordeaux **7** (1995), 219–254.

[10] Daniel Shumow, *Isogenies of elliptic curves: a computational approach*, Masters Thesis, Department of Mathematics, University of Seattle, Seattle, WA, (June 2009).

[11] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd Edition, Springer-Verlag, Graduate Texts in Mathematics, (2009).

[12] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, Graduate Texts in Mathematics, (1999).

[13] Lawrence C. Washington, *Elliptic curves: number theory and cryptography*, 2nd Edition, Chapman & Hall, (2008).