ISOGENIES. 28.03.2022.

- isogenies are homomorphisms. Many results of WEEK 3 apply. (and WEEK 4).
  - degree, separable, non-separable, kernel, etc.

$\phi : E_1 \longrightarrow E_2$ is a mapping

$$\phi : (x_1, y_1) \longmapsto \left(\phi_x(x_1, y_1), \phi_y(x_1, y_1) \right)$$

where ϕ_x, ϕ_y satisfy the equation of E_2: $\phi_y^2 = \phi_x^3 + A_2 \phi_x + B_2$ in shortW.

ϕ_x, ϕ_y can have coefficients in an extension of K.

- Automorphisms of E form a GROUP $AUT(E)$ under composition
- Homomorphisms $E_1 \to E_2$ form a $\mathbb{Z}$-module $Hom(E_1, E_2)$ under addition
- Endomorphisms of E form a RING $End(E)$ under addition and composition.

Over a finite field, we always have scalar multiplication $[m]$, $m \in \mathbb{Z}$, and Frobenius π_q,

$$\mathbb{Z}[\pi_q] \subset End(E).$$

Remember DIVISION POLYNOMIALS: § 3.2 p80 in Washington. Theorem 3.6.

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

The roots of $\psi_m(x)$ are the x-coordinates of the points of order (dividing) m.
$\psi_m(x)$ has degree $(m^2-1)/2$ when m is odd (LEMMA 3.5 p 82 in Washington).
→ to find a point of m-torsion, one computes the roots of $\psi_m(x)$. (in K or in an extension).

$E : y^2 = x^3 + Ax + B$ an elliptic curve defined over a field K.

The FUNCTION FIELD of E is

$$K(E) = K(x)[y]/(y^2 - (x^3 + Ax + B))$$

of transcendence degree 1 (i.e. there is one free variable of degree as large as desired, x).

$\frac{1}{y} = \frac{y}{y^2} = \frac{y}{x^3 + Ax + B}$ so we can invert y.

HOMOMORPHISMS: $\phi : E \to E'$ such that $\phi(O_E) = O_{E'}$, it preserves the neutral.

ISOGENIES are NON-ZERO HOMOMORPHISMS.

Same definitions of degree and kernel as in CHAPTER 2 Section 2.9.

ϕ is an isogeny from E_1 to E_2 given by rational functions

$$\phi = \left(r_1(x),\ y \cdot r_2(x) \right), \quad r_1, r_2 \text{ rational functions in } x.$$

Write $r_1(x) = \frac{n(x)}{d(x)}$ numerator with $\gcd(n,d) = 1$
denominator (coprime polynomials in x).

DEGREE $\deg(\phi) = \max(\deg(\text{numerator}), \deg(\text{denominator}))$ d-isogeny

SEPARABLE if the derivative $n'(x)$ is not zero

NOT SEPARABLE. otherwise, for example when it's a p-power, where $p = \text{char}(K)$.

Example: a 2-isogeny, a 3-isogeny.

do it after page 4.

Vélu's formulas for 2-isogenies.

Let $(x_0, 0)$ be a 2-torsion point on $E: y^2 = x^3 + Ax + B$.

Set $t = 3x_0^2 + A$. Then

$$(x,y) \mapsto (u,v) = \left(\frac{x^2 - x_0 x + t}{x - x_0},\ y\,\frac{(x-x_0)^2 - t}{(x-x_0)^2} \right)$$

defines a normalized separable isogeny from E to E':

$$E': y^2 = x^3 + (A - 5t)x + (B - 7x_0 t)$$

In Montgomery form: Example 12.3 in Washington, p 388.

$E: y^2 = x^3 + a_2 x^2 + a_4 x$, and $P_2 = (0,0)$ has order 2.

Kernel $\{\mathcal{O}, (0,0)\}$.

$$\phi_2: E \to E': \quad y'^2 = x'^3 - 2a_2 x'^2 + (a_2^2 - 4a_4)x'.$$

$\neq 0$ otherwise singular

$$(x,y) \mapsto \begin{cases} \mathcal{O} & \text{if } P(x,y) = (0,0) \\ \left(x + a_2 + \frac{a_4}{x},\ y\left(1 - \frac{a_4}{x^2}\right)\right) & \text{otherwise.} \end{cases}$$

The curves have DISTINCT j-invariant:

$$j(E) = 2^8 \frac{(3a_4 - a_2^2)^3}{(4a_4 - a_2^2)a_4^2} \quad \text{and} \quad j(E') = 2^4 \frac{(a_2^2 + 12a_4)^3}{(4a_4 - a_2^2)^2 a_4}$$

still the curves have the same order.

if ϕ is a separable isogeny, then $\deg \phi = \#\ker \phi$.
if ϕ is not separable (and non-zero), then $\deg \phi > \#\ker \phi$.

non-separable: consider a quadratic extension, ex. $\mathbb{Q}(i) \hookrightarrow \mathbb{F}_{p^2}$

$p \equiv 3 \bmod 4$, $\mathbb{F}_p = GF(p)$, and $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2+1)$.

$E: y^2 = x^3 + (a_0+ia_1)x + (b_0+b_1 i)$.

$E^p: (y^2)^p = (x^3)^p + (a_0+a_1 i)^p x^p + (b_0+b_1 i)^p$

$(y^p)^2 = (x^p)^3 + (a_0 + a_1 i^p)\, x^p + (b_0 + b_1 i^p)$

and $i^p = i^{p-1} i = (i^{\frac{p-1}{2}})^2 \cdot i = (i^2)^{\frac{p-1}{2}} \cdot i = (-1)^{\frac{p-1}{2}} \cdot i$.

Remember that $(-1)^{\frac{p-1}{2}}$ is the Legendre symbol $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,
here we assumed that -1 is not a square (indeed $p \equiv 3 \bmod 4$),
hence $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$.

Finally, $i^p = -i$ and $E^p: y'^2 = x'^3 + (a_0 - a_1 i)x' + (b_0 - b_1 i)$.

$\phi_p: E \to E^p$
$(x,y) \mapsto (x^p, y^p)$ is a degree p non-separable isogeny.

Prop 12.8 & 12.9.

- $\ker(\phi)$ is a finite subgroup of $E(\bar{K})$.
- ϕ is surjective: $\forall Q \in E'(\bar{K})$, $\exists P \in \bar{K}$, $\phi(P) = Q$, where $\bar{K}$ means any (algebraic closure) extension of K

Prop 12.12.

$$E_1 \xrightarrow{\phi_2} E_2, \quad E_1 \xrightarrow{\phi_3} E_3$$

ϕ_2, ϕ_3 isogenies, E_1, E_2, E_3 elliptic curves defined over K.

if $\ker(\phi_2) = \ker(\phi_3)$, then E_2 is isomorphic to E_3 over $\bar{K}$.
in fact, there is an isomorphism $\beta: E_2 \to E_3$ such that $\beta \circ \phi_2 = \phi_3$.

THEOREM 12.14. DUAL ISOGENY.

Let $\phi: E_1 \to E_2$ be an isogeny of elliptic curves. Then there exists a DUAL ISOGENY $\hat{\phi}: E_2 \to E_1$ such that $\hat{\phi} \circ \phi$ is multiplication by $\deg \phi$ on E.
(and $\phi \circ \hat{\phi}$ is multiplication by $\deg \phi = \deg \hat{\phi}$ on E_2).

PROOF of the dual isogeny.

Assume that the degree is coprime to the characteristic of the field.

See (Silverman, GTM106 for a proof in the general case).

Remember: multiplication-by-m map $[m]$ has degree m^2 and kernel the m-torsion points.

Let $N = \deg \phi$ coprime to $\mathrm{char}(K)$.

Then $\ker(\phi) \subseteq E_1[N]$ because $\ker(\phi)$ is a subgroup of E_1 of order N.

(but $\#E_1[N] = N^2$ so $\ker(\phi)$ is not all $E_1[N]$).

and the image of $E_1[N]$ under ϕ is a subgroup of E_2 of order N.

this is E_2 not E_1, typo in Washington's book.

$$E_1 \xrightarrow{\phi} E_2$$

$E_1[N]$ has order N^2, N points are in the kernel of ϕ:

$\#\,\phi(E_1[N]) = N$ in E_2.

Vélu's formulas (Th. 12.16 in Washington) provide a way to compute an isogeny of prescribed kernel

$$\phi_2 : E_2 \longrightarrow E_3 \quad \text{such that } \ker(\phi_2) = \phi(E_1[N])$$
$$\Rightarrow \#\ker(\phi_2) = N.$$

Then composing ϕ and ϕ_2: $\phi_2 \circ \phi$ has kernel $E_1[N]$.

The multiplication-by-N map $[N]$ has the same kernel $E_1[N]$ as $\phi_2 \circ \phi$.

By Prop. 12.12 previous page, there is an isomorphism $\beta : E_3 \to E_1$ such that $\beta \circ \phi_2 \circ \phi$ is $[N]$. Let $\hat{\phi} = \beta \circ \phi_2$. □.

Remark. If we choose a different kernel for ϕ_2: not $\phi(E_1[N])$ but OTHER points of order N, then we do not land to E_1 back, E_3 is a new curve with a new (distinct) j-invariant. This is used in isogeny graph and post-quantum cryptography.

If E_1 has order $2^n \cdot c$, for some high power n, we can chain the curves

$$E_1 \longrightarrow E_2 \longrightarrow E_3 \longrightarrow E_4 \longrightarrow \dots \longrightarrow E_n.$$

But: this is hard to generate a curve with smooth order (if ordinary).

if E and E' are in short Weierstrass form, then every separable isogeny $\phi : E \to E'$ can be expressed as a rational map

$$\phi : (x,y) \mapsto \left(f(x), \lambda\, y\, \frac{df}{dx}(x) \right)$$

↖ derivative of f with respect to x.

for some function f in the function field $\bar{K}(E)$ $\bar{K}(x)$ and some twisting factor λ of $\bar{K}$.

The isogeny is normalized if $\lambda = 1$.

Quotient isogenies

If ϕ is an isogeny, then $\ker \phi$ is a finite subgroup of $E(\bar{K})$.

Conversely, if S is a finite subgroup of $E(\bar{K})$, then there exists a separable quotient isogeny

$$\phi : E \to E/S \quad \text{with} \quad \ker \phi = S.$$

E/S is defined up to isomorphism, but is unique if we require $\lambda = 1$ (normalized ϕ).

→ Velu formulas give ϕ and E/S.

→ Separable isogenies are determined, up to isomorphism, by their kernel.

Velu for degree 2 → example on page 2.

Odd-degree Velu. Section 12.3.

Let $G \subset E$ be a finite subgroup of odd order.

For example: choose P of odd order n in $E(K)$ and set $G = \langle P \rangle$ to be generated by P. $d = 3$, and P a 3-torsion point for ex.

For each $Q = (x_Q, y_Q) \neq O$ in G, set $t_Q = 3x_Q^2 + A$, $u_Q = 2y_Q^2$, $w_Q = u_Q + y_Q x_Q$

Now set $t_G = \sum_Q t_Q$, $w_G = \sum_Q w_Q$, and

$$f(x) = x + \sum_Q \frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2}$$

Then $(x,y) \mapsto (f(x),\ y f'(x))$ defines a normalized separable isogeny

$$E \to E' : \quad y^2 = x^3 + (A - 5t_G)x + (B - 7w_G)$$

with kernel G.

Examples.

- Sage Math $p = 2^{127} - 1$, $E: y^2 = x^3 + 40x^2 + x \ / \mathbb{F}_p$

  $\#E = 2^7 \cdot 3^7 \cdot 7 \cdot c$ for some prime c.

  We can do a walk

- BLS12-381. $y^2 = x^3 + b$ has j-invariant 0.

  The kush-map Elligator for example does not work.

  Use a 2-isogeny to move to another curve $j' \neq 0$ such that common hash-maps are available.