The geometry of efficient arithmetic on elliptic curves

I Models of Elliptic Curves
  What is an elliptic curve?
II Arithmetic
  A. Addition morphism
  B. Doubling morphism = Isogeny Isogenies
  C. Scalar multiplication (A+B)
  as. Montgomery morphism (deconstructing)
III. Explicit examples
  A. Hessian normal form
  B. Split μ_4-normal form
IV. Generalizations (PHS) (NO TIME)

Models of elliptic curves

What is an elliptic curve?

(E,O) $(k(E), m_O)$ $E_0 \subset \mathbb{A}^2, (x_0,y_0)$ or $m=\infty$

give sufficient $f(x,y)=0$
  data, but insufficient as
  computational model.

1) Need a coordinate system in which to express arithmetic
2) Need a nonsingular model or at least $E(k)$ nonsingular
3) Need a projective model or at least $E(k) \subseteq E_0(k)$.

This motivates the study of a triple $(E, \iota: E \hookrightarrow \mathbb{P}^r, O)$.

Models

A model of an elliptic curve E is a projective embedding $E \to \mathbb{P}^r$ as a member of a family

$$\begin{array}{ccccc} E & \to & \mathcal{E} & \hookrightarrow & \mathbb{P}^r_S = \mathbb{P}^r \times S \\ \downarrow & & \downarrow & & \downarrow \\ \{t\} & \to & S & = & S \end{array}$$

E.g. $\mathcal{E}: Y(Y+aX+bZ)Z = X^3 \subseteq \mathbb{P}^2$ a family over $S = \mathbb{A}^2 \setminus \{\text{disc}(a,b)=0\}$,

OR

$\mathcal{E}: X_0^2 - X_2^2 = c^2 X_1 X_3 \quad O=(c:1:0:1)$
$\quad X_1^2 - X_3^2 = c^2 X_0 X_2$ in $\mathbb{P}^3$ over $S \subseteq \mathbb{A}^1$.

OR

$\mathcal{E}: X^3+Y^3+Z^3 = dXYZ$, $O=(0:1:-1)$ in $\mathbb{P}^2$

Often we identify the family with its generic fiber — an elliptic curve over the function field $k = k(S)$.

Hypothesis:

We assume E is embedded in $\mathbb{P}^r$ by a complete linear system:

Set D to be the divisor cut out by $X_0 = 0$, and $x_0 = 1, x_1, \dots, x_r$ a basis for the Riemann-Roch space

$$L(D) = \{f \in k(E) \mid \text{div}(f) + D \geq 0\}$$

such that

$$\begin{array}{ccc} E & \xrightarrow{\iota} & \mathbb{P}^r \\ P & \longmapsto & (x_0(P) : \dots : x_r(P)) \end{array}$$

is the given embedding.

Symmetric embeddings

We moreover assume that the embedding is such that $[-1]$ is given by a linear transformation.

Equivalent conditions:
- $[-1]^* D \sim D$
- $D = \sum(P_i)$ then $\sum P_i \in E[2]$
- $[-1]$ acts linearly.

Defn Symmetric embedding. E.g. $D = \sum_{T \in G}(T)$.

Consequently, the cost of negation is negligible.

Action of Torsion

Lemma Translation by a torsion point T is ~~linear~~ given by a linear transformation on $E \subseteq \mathbb{P}^r$ iff $T \in E[d]$, where $d \in (r+1)$ is the embedding degree ($d = \deg D$).

N.B.
The class of the embedding is determined by $d = \deg D$ and $T = eval(D) = \sum P_i \in E(k)$, up to linear isomorphism.

E.g.

Cubic curves in $\mathbb{P}^2$:	Quartic curves in $\mathbb{P}^3$
$E[3] \subseteq E(k)$ acts linearly	$E[4] \subseteq E(k)$ acts linearly

Special constructions

- $\mu_\ell \subseteq E[\ell]$ acting by coordinate scaling by roots of unity $(X_i) \mapsto (\zeta_\ell^i X_i)$
- $\mathbb{Z}/\ell\mathbb{Z} \subseteq E[\ell]$ acting by cyclic coordinate permutation $(X_0, \ldots, X_r) \mapsto (X_1, \ldots, X_r, X_0)$.
- $D = \sum_{T \in G}(T) \subseteq E[\ell]$.

II Arithmetic

Addition Morphism

$(P,Q) \longmapsto P+Q$

The addition morphism $\mu: E \times E \to E$ is uniquely determined by (E,O). Given an embedding $E \subseteq \mathbb{P}^r$ a tuple $(f_0,\dots,f_r)$ of bihomogeneous polynomials in

$$k[E] \otimes_k k[E] = \frac{k[X_0,\dots,X_r]}{I_E(X)} \otimes \frac{k[Y_0,\dots,Y_r]}{I_E(Y)}$$

which defines μ on the complement of its exceptional set

$$V(f_0,\dots,f_r) \cap E \times E$$

is called an <u>addition law</u>. If nonzero, the exceptional set is a nonzero divisor on $E \times E$. In particular, no addition law determines μ everywhere (over k). On the other hand, the exceptional set can have no k-rational point, said to be <u>arithmetically complete</u>. If $(f_0,\dots,f_r)$ and $(g_0,\dots,g_r)$ are addition laws of the same bidegree, then so is their sum. In particular, the set of addition laws of given bidegree form a vector space.

<u>N.B.</u>

The dimension of this space is:

- 0 if $(2,2) \not\leq (m,n)$
- 1 if $(2,2) = (m,n)$
- $2(m-1)(n-1)-1$ if $(2,2) < (m,n)$

In particular the critical case is $(m,n)=(2,2)$, also most interesting for computation.

Note: we seek to minimal the number of multiplications of monomials. We assume additions and scalar multiplications are negligible.

Heuristics for addition laws of bidegree (2,2), $d = r+1$.

Input $(X_0,\dots,X_r), (Y_0,\dots,Y_r)$

$X_{ij} = X_i X_j,\ 0 \le i \le j \le r$ AND $Y_i Y_j,\ 0 \le i \le j \le r$

$\binom{d+1}{2} - m = 2d$ $\qquad$ $\binom{d+1}{2} - m = 2d$

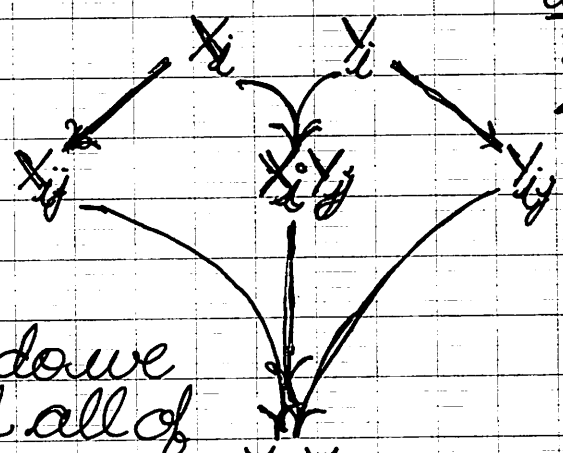
$m = \dim(I_E \cap k[X_0,\dots,X_r]_2)$ $\qquad$ ↑ Riemann–Roch $= \deg(2D)$

E.g. $d=3$: $m=0$ and there are no relations of degree 2.

$d=4$: $m=2$ and, up to the two quadratic relations we can choose 8 out of 10 monomials to span $\underline{k[X_0,\dots,X_r]_2}$.
I_E

OR compute $X_i Y_j,\ 0 \le i,j \le r$: d^2 products.

Constructing all biquadratic monomials requires $4d^2 + 4d$ products for $4d^2$ monomials. $= 4d(d+1)$



But, do we need all of these multiplications? All of these monomials?!

$d=3$:
36 monomials
48 multiplications

$d=4$:
64 monomials
80 mults

Naïve eval on a generic curve will.

Structured models, structured algorithms

Assume now that $E \subseteq \mathbb{P}^r$ is such that μ_E ↷ E by coordinate scaling by roots of unity ($X_i \to \zeta_d^i X_i$)

Ex. $X_0^3 + X_1^3 + X_2^3 = dX_0X_1X_2 \subset \mathbb{P}^2$ Hessian normal form

$X_0^2 - X_2^2 = c^2 X_1 X_3 \subseteq \mathbb{P}^3$
$X_1^2 - X_3^2 = c^2 X_0 X_2$ Split μ_3-normal form.

N.B $d = r+1$, acts linearly.

Under this hypothesis, noting that $\mu(P+T, Q-T) = \mu(P,Q)$, we can decompose the space of biquadratic polynomials into eigenspaces

$d=3$. The 36 dim space eigen decomposes into 12 dim spaces. In fact, the 9 dim space of bilinear forms $\mathrm{Span}(\{X_iY_j\}) = V$ decomposes as

$V = V_0 \oplus V_1 \oplus V_2$ where $V_0 = \{X_0Y_0, X_1Y_1, X_2Y_2\}$
$V_1 = \{X_0Y_2, X_1Y_0, X_2Y_1\}$
$V_2 = \{X_0Y_1, X_1Y_2, X_2Y_0\}$

Then $\mathrm{Sym}^2 V_0 + V_1 \otimes V_2$ surjects on the eigenspace of $\mathbb{1}$ in biquadratic forms.

Each of V_i requires 3M, $\mathrm{Sym}^2 V_0$ at most 6M and $V_1 \otimes V_2$ at most 9M, but the space is at most 9 dim! Each M is either already known or enlarges the span of the subspace spanned by monomials, hence at most 9M are required once V is computed.

$d=4$

The space of bilinear forms has dimension 16: $V = V_0 \oplus V_1 \oplus V_2 \oplus V_3$

$V_0 = \langle x_0 y_0, \ldots, x_3 y_3 \rangle$

etc.

The 4 dim'l space of biquadratics consists of 4 eigenspaces of ~~size~~ dim 16

This motivates the study of addition eigenforms $(f_0, \ldots, f_r)$.

It is worth noting that

$\mathrm{Span}(f_0, \ldots, f_r)$

is a dim $r+1 = d$ inside a space of dim $4d^2$, and an eigenform lies inside ~~a space~~ an eigenspace (for $\mathbb{Z}/d$) of dimension $4d$.

Optimally we would like to compute a monomial basis of $\mathrm{Span}(f_0, \ldots, f_r)$ with $2d$ mults!

Isogenies (Doubling or Tripling or...)
Consider the example of a μ_ℓ-oriented model, $[\ell]=[2]$ or $[3]$, and $[\ell]=\phi\psi$, with $\psi(X_0,\dots,X_r)=(X_0^\ell,\dots,X_r^\ell)$ on E/μ_ℓ.
How do we compute ϕ efficiently?

Evaluation of morphisms.
Assume $C_1\subseteq\mathbb{P}^r$, $C_2\subseteq\mathbb{P}^s$ and $\phi: C_1\to C_2$ is determined by $(f_0,\dots,f_s)$ where $\deg\phi=\deg f_i=\ell$.
Set $V_1=I_{C_1}\cap k[X_0,\dots,X_r]_\ell$ and $V_s=V_1+\langle f_0,\dots,f_s\rangle$.

Lemma
If $C_2\subseteq\mathbb{P}^s$ is given by a complete linear system of degree $s+1$, then $\dim(V_s/V_1)=s+1$.

Proof. C_2 is not contained in a hyperplane. □

Then... Construct a flag
$$V_1\subsetneq V_0\subsetneq V_1\subsetneq\cdots\subsetneq V_s$$
using a minimal number of multiplications for each V_{i+1} over V_i.
Expected complexity:
$$c\log_2(\ell)(s+1)M.$$

Remarks
Given an isogeny $\phi: E_1\to E_2$ of degree ℓ, there exist embeddings $E_i\subseteq\mathbb{P}^r$ (of the same degree) such that ϕ is given everywhere by a tuple of polynomials of degree ℓ.

Example

There does not exist a tuple of quadratic polynomials determining a separable isogeny of degree 2 between elliptic curves in $\mathbb{P}^2$.

Counter-example?

$E_1 : y^2 = x(x-1)^2 + a^2x^2 \longrightarrow E_2 : y^2 = x(x+2a)^2 + (a-2)^2x^2$

$(X,Y,Z) \longmapsto (4a^2X(X-Z),\ 4a^2Y(X+Z),\ Y^2 - a^2X^2 - (X-Z)^2)$

$(0:1:0) \longmapsto (0:0:1)$

Not a contradiction — composition of an isogeny with a translation by the 2-torsion point $(0:0:1)$.

Otherwise a complete system is given by a pair of tuples of degree 3 polynomials.

Scalar multiplication

Achieved by a double and add algorithm, combining the above algorithms.

N.B.

I'm glossing over windowing and multibase methods.

Next we describe how to carry out scalar multiplication as a composition of a conjugate doubling morphism.

Montgomery morphism (aka deconstructing scalar multiplication)

Notation $P \in E(k)$ fixed.

$\mathcal{K} = \mathcal{K}(E) = E/\langle \pm 1 \rangle \ (\cong \mathbb{P}^1)$

$\mathcal{K}(E \times E) = E \times E / \langle (-1,-1) \rangle \longrightarrow \mathcal{K} \times \mathcal{K}$

N.B. Can replace E by any Jacobian or abelian variety.

Idea: Use a P-oriented model for E inside $\mathcal{K} \times \mathcal{K} \ (\cong \mathbb{P}^1 \times \mathbb{P}^1)$ on which we can efficiently compute scalar multiples of P.

Setup $\begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$

$\phi : E \times E \longrightarrow E \times E$

$(Q,R) \longmapsto (2Q, Q+R)$

– an isogeny of abelian varieties which is an elementary step in a double and always add algorithm

$\tau : E \times E \longrightarrow E \times E$

$(Q,R) \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \to (-R,-Q)$

such that $\tau\phi\tau(Q,R) = (Q+R, 2R)$.

Moreover define

$\delta : E \times E \longrightarrow E$ and $\Delta_P = \delta^{-1}(P)$

$(Q,R) \longmapsto Q - R$ $\quad = \{(Q, Q-P)\}$

Scalar multiplication $(n,P) \longmapsto nP$

Write $n = n_t \cdots n_1 n_0$, $\phi_1 = \phi$, $\phi_0 = \tau\phi\tau$.

$(Q,R) = (P,O)$

for $i = t \ldots 0$:

if $n_i = 1$: $(Q,R) \leftarrow \phi_1(Q,R) = (2Q, Q+R)$

if $n_i = 0$: $(Q,R) \leftarrow \phi_0(Q,R) = (Q+R, 2R)$

return R.

Additional notation:
$\mathcal{K}(X)$ = image in $\mathcal{K}(A)$ of $X \subseteq A$.

First key observation
$\phi(\Delta_P) = \Delta_P$ & $\tau(\Delta_P) = \Delta_P$ so these isogenies induce morphisms
(ϕ an isogeny fixing the origin $(0,P)$ and τ an isomorphism $[-1] \circ \tau_P$).

Second key observation
$$\begin{array}{ccc} E\times E & \xrightarrow{\phi} & E\times E \\ \downarrow & & \downarrow \\ \mathcal{K}(E^2) & \xrightarrow{\phi} & \mathcal{K}(E^2) \end{array}$$
- ϕ extends to $\mathcal{K}(E^2)$ but not to $\mathcal{K}\times\mathcal{K}$
- τ extends to $\mathcal{K}^2$.

of curves

BUT the restriction to $\mathcal{K}(\Delta_P)$ induces $\mathcal{K}_P^2 \xrightarrow{\phi} \mathcal{K}_P^2 = \mathcal{K}(\Delta_P) \subseteq \mathcal{K}^2$.
In particular, ϕ on the first coordinate is $[2]$ on the Kummer line, and the second coordinate arises from $(P, Q, R = \overline{Q-P}) \longmapsto \overline{Q+P}$.
$\{P\}$ $\longleftarrow \mathcal{K}\times\mathcal{K}$

Third key observation: if $P \notin E[2]$
$$\begin{array}{ccccccc} E & \xrightarrow{\simeq} & \Delta_P & \xrightarrow{\simeq} & \mathcal{K}(\Delta_P) & \xrightarrow{\simeq} & \mathcal{K}_P^2 \\ [2]\downarrow & Q & \| & \nearrow\tau & \| & \nearrow\tau & \downarrow \phi \\ E & & \Delta_P & & \mathcal{K}(\nabla_P) & & \mathcal{K}_P^2 \end{array} \qquad E \cong \mathcal{K}_P^2 \quad (Q, \overline{Q-P})$$
$$2Q \qquad (\overline{2Q}, \overline{2Q-P})$$

ϕ is thus
- well-defined
- efficient
- induces a skew $[2]$

cf. Ben's talk for $g=2$

The algorithms for $g=1,2$ are known (in families with certain structure).
The algorithms for Point recovery, inverting $E \longrightarrow \mathcal{K}_P^2$ complete the picture.

Denote $\tau(X_0, X_1, \dots, X_r) = (X_0, \zeta X_1, \dots, \zeta^r X_r)$.

Hessian normal form: Addition law evaluation

$X_0^3 + X_1^3 + X_2^3 = dX_0X_1X_2$, $O = (0,1,-1)$.

An eigenform:

$(f_0, f_1, f_2) = (X_0^2Y_1Y_2 - X_1X_2Y_0^2,\ X_2^2Y_0Y_1 - X_0X_1Y_2^2,\ X_1^2Y_0Y_2 - X_0X_2Y_1^2)$

invariant under $\tau \times \tau^{-1}$.

$V_X = \langle X_0, X_1, X_2 \rangle$, $V_Y = \langle Y_0, Y_1, Y_2 \rangle$

$\mathrm{Sym}^2(V_X) = \langle X_0^2, X_1X_2 \rangle \oplus \langle X_0X_1, X_2^2 \rangle \oplus \langle X_0X_2, X_1^2 \rangle$

$\mathrm{Sym}^2(V_Y)$

$V_X \otimes V_Y = V_0 \oplus V_1 \oplus V_2$

$V_0 = \langle X_0Y_0, X_1Y_1, X_2Y_2 \rangle$ 3M

$V_1 = \langle X_1Y_0, X_2Y_1, X_0Y_2 \rangle$ 3M

$V_2 = \langle X_0Y_1, X_1Y_2, X_2Y_0 \rangle$ 3M

(6M)

$\langle f_0, f_1, f_2 \rangle \subseteq V_1 \otimes V_2 \hookrightarrow \mathrm{Sym}^2(V_X) \otimes \mathrm{Sym}^2(V_Y)$

dim 3 — dim 9 — dim 36

9M — (eigenspace dim 12)

In fact we can compute the target space $\langle f_0, f_1, f_2 \rangle$ as a subspace of the six dim'l space ($= 6M$)

$\langle X_0Y_1 \circ X_0Y_2,\ X_1Y_0 \circ X_2Y_0,$
$X_2Y_0 \circ X_2Y_1,\ X_0Y_2 \circ X_1Y_2,$
$X_1Y_0 \circ X_1Y_2,\ X_0Y_1 \circ X_2Y_1 \rangle$

(We would really like to do 3M, not 6M, to construct a space of dim 3.)

Can only hope to build 2Δ w/o taking differences.

Net complexity: 12M.

What went wrong?

Why do we need to compute a 6 dim'l space?

The exceptional divisor is 3Δ.

The ~~exceptional~~ divisor of act. by the forms $\langle X_0Y_1 - X_1Y_0, X_0X_2 - X_2Y_0, \dots \rangle$ is Δ.

Odd vert $(P,Q) \leftrightarrow (Q,P)$.

Split μ_4-normal form.

$\mathcal{E}: X_0^2 - X_2^2 = c^2 X_1 X_3 \quad O = (c:1:0:1)$

$X_1^2 - X_3^2 = c^2 Y_0 X_2 \quad S = (0:1:c:1)$

An eigenform: $T = (c:i:0:-i)$

$(X_0^2 Y_0^2 - X_2^2 Y_2^2 ; c(X_0 X_1 Y_0 Y_1 - X_2 X_3 Y_2 Y_3), X_1^2 Y_1^2 - X_3^2 Y_3^2,$
$c(X_0 X_3 Y_0 Y_3 - X_1 X_2 Y_1 Y_2))$

invariant under $\tau \times \tau^{-1}$.

N.B. The exceptional divisor is $\Delta_S + \Delta_R + \Delta_{S+T} + \Delta_{S-T}$

$V = V_X \otimes V_Y \supseteq V_0 = V^{\tau \times \tau^{-1}} = \langle X_0Y_0, X_1Y_1, X_2Y_2, X_3Y_3 \rangle$

dim 16 dim 4

σ 4M

$= V^+ \oplus V^-$ for $\sigma \times \sigma$

$f_0 = (X_0Y_0 + X_2Y_2)(X_0Y_0 - X_2Y_2)$

$f_2 = (X_1Y_1 + X_3Y_3)(X_1Y_1 - X_3Y_3)$

$V^+ \qquad V^-$

and

$\frac{1}{c}(f_1 + f_3) = (X_1Y_1 + X_3Y_3)(X_0Y_0 - X_2Y_2)$

$\frac{1}{c}(f_1 - f_3) = (X_0Y_0 + X_2Y_2)(X_1Y_1 - X_3Y_3)$

4M to construct $\langle f_0, f_1, f_2, f_3 \rangle = V^+ \otimes V^-$.

The divisor cut out

by $V^+ = \langle X_0Y_0 + X_2Y_2, X_1Y_1 + X_3Y_3 \rangle$ is $\Delta_{S+T} + \Delta_{S-T}$

by $V^- = \langle X_0Y_0 - X_2Y_2, X_1Y_1 - X_3Y_3 \rangle$ is $\Delta_S + \Delta_R$

Hence $V^+ \otimes V^-$ cuts out the exact divisor and we compute the minimal 4-dimℓ space required.

$R = S + 2T$

IV Generalizations of elliptic curves. Principal homogeneous spaces

$\mu : E \times E \to E$	$\mu : E \times X \to X$
$[l] : E \to E$	? $[l] : X \to E$ (fixed l)
$\delta : E \times E \to E$	$\delta : X \times X \to E$
$[-1] : E \to E$	no inversion

X = genus one curve w/ Jacobian E.

El Gamal

$(P, Q = kP) \in E \times E$

$M \longmapsto (lP, M + lQ) \in E \times X$

$= (R, S)$

$M = \delta(S, kR) = (M + lQ) - kR \in X.$

Diffie–Hellman

$(P, Q) \in E \times X$ (Public)

Exchange $R = Q + kP$, $S = Q + lP$ — Justifiable only if exponentiation is fast ($[2]$ on E, μ on $E \times X$)

Compute

$\delta(R, Q) = kP$

$\delta(S, Q) = lP$

then $Q + klP$ is the secret.

Double and add in a PHS

Compute $Q + kP$ where $k = 2k_1 + k_0$

$Q_1 = Q + k_0 P$

$P_1 = 2P$

then compute $Q_1 + k_1 P_1$.

Problems:

No windowing (works with higher level bits)

No Montgomery multiplication.