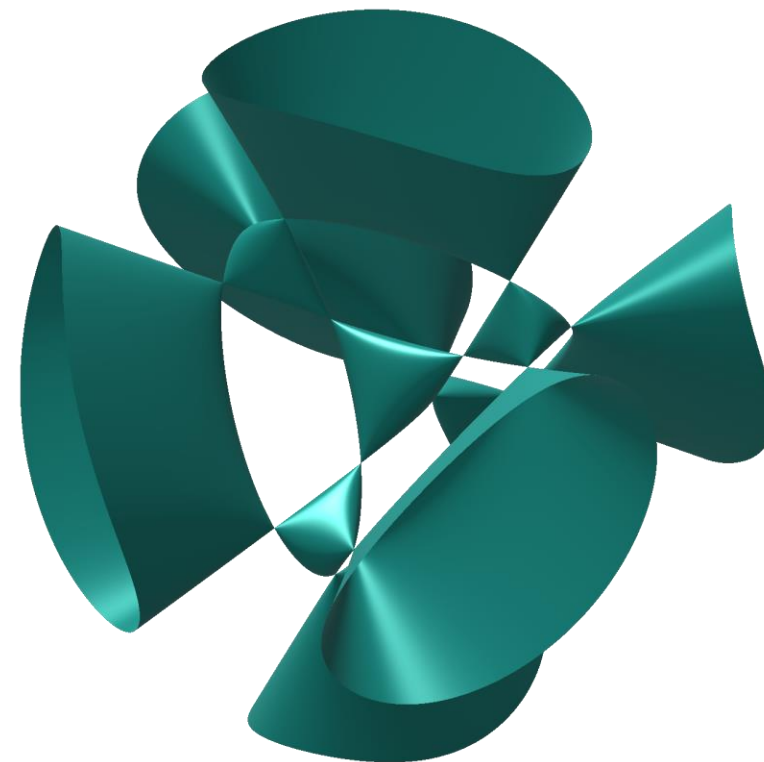


An introduction to hyperelliptic curve cryptography

Divisors, Jacobians and Kummer surfaces

Craig Costello

Workshop on Elliptic Curves
Sydney, 1 October 2026



The cryptographic question

Alice

Public generator G

Bob

a

b

$[a]G$

$[b]G$

$[ab]G$

shared element

$[ab]G$

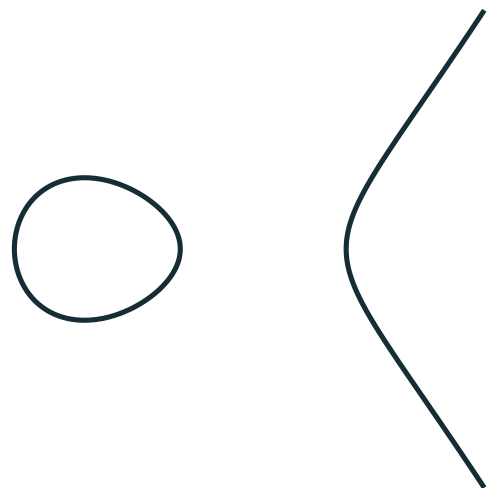
$$A = [a]G, \quad B = [b]G$$

$$[a]B = [b]A = [ab]G$$

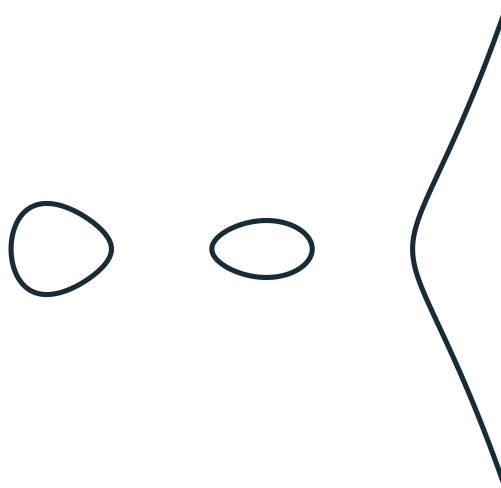
Public multiples are easy to compute.

Recovering the secret scalar should be hard.

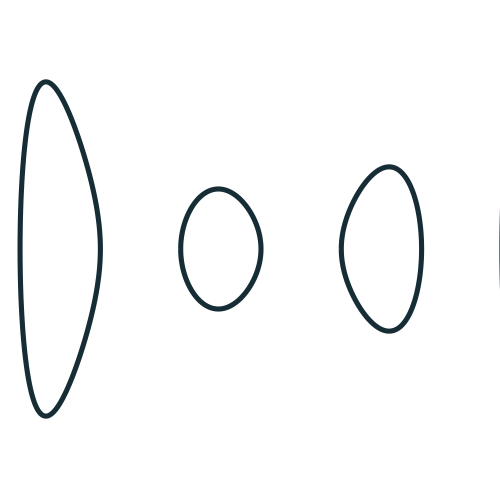
A larger family of curves



genus 1



genus 2



genus 3

$$C_g: y^2 = f(x), \quad \deg f = 2g + 1$$

Odd characteristic and squarefree f .
One point at infinity in this model.

The new group elements

In genus 2, a typical element needs two points.

$$(P) + (Q) - 2(\infty)$$

Addition will combine collections, then reduce them.

Divisors give those collections a precise meaning.

Divisors

2



P

-3



Q

1



R

-1



S

A point may occur with a positive or negative coefficient.

$$D = \sum_P n_P(P), \quad n_P \in \mathbb{Z}$$

Integer multiplicities, with only finitely many nonzero coefficients.

Parentheses mark a formal point symbol.

Adding signed collections

$$D_1 = 2(P) - 3(Q)$$

$$D_2 = 3(Q) + (R) - (S)$$

$$D_1 + D_2 = 2(P) + (R) - (S)$$

Coefficients add. Matching positive and negative contributions cancel.

Degree zero

Positive multiplicities

$$(P) + (Q)$$

$$+2$$

Negative multiplicities

$$-2(\infty)$$

$$-2$$

total degree 0

$$\deg D = \sum_P n_P$$

$$\deg((P) + (Q) - 2(\infty)) = 0$$

Degree zero means the multiplicities balance.

A function leaves a divisor

Zeros

$$(P) + (\bar{P})$$

$$+2$$

Poles

$$-2(\infty)$$

$$-2$$

Example: $h = x - x(P)$

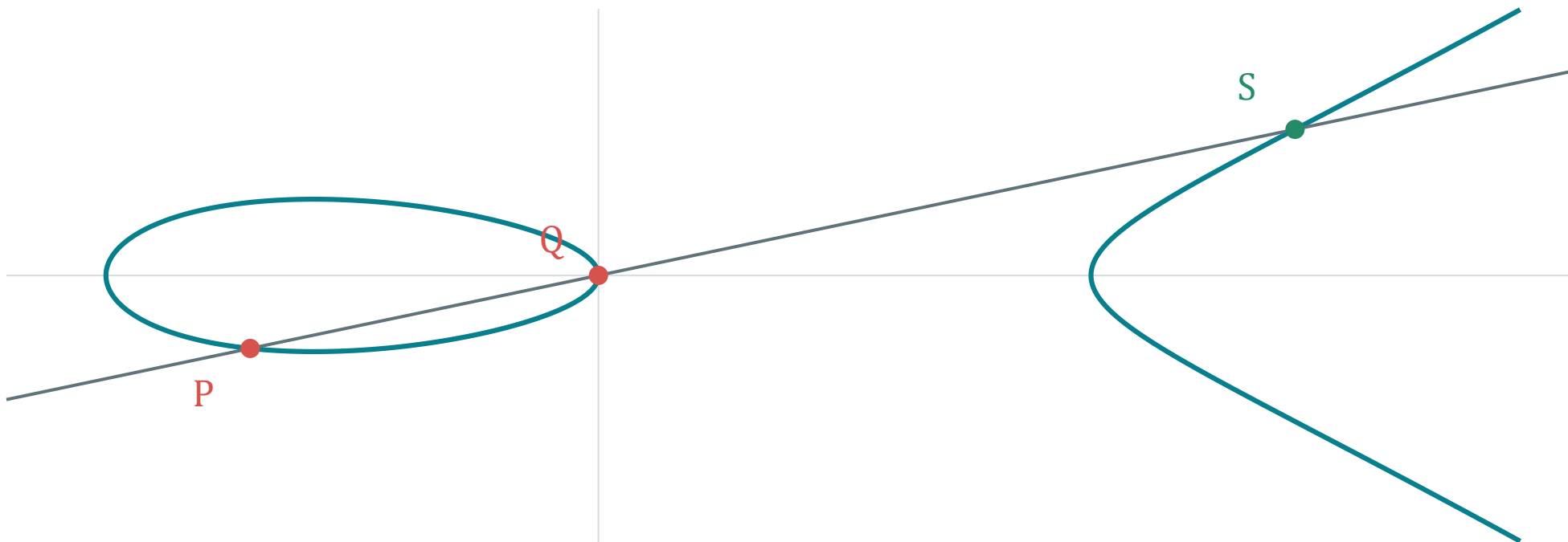
$$\operatorname{div}(h) = \sum_P \operatorname{ord}_P(h)(P)$$

$$\deg \operatorname{div}(h) = 0$$

Zeros contribute positive multiplicities.

Poles contribute negative multiplicities.

The familiar line intersection



$$\operatorname{div}(\ell) = (P) + (Q) + (S) - 3(\infty)$$

Three intersections, counted with multiplicity.

Products become sums

$$\operatorname{div}(h_1 h_2) = \operatorname{div}(h_1) + \operatorname{div}(h_2)$$

$$\operatorname{div}(h_1/h_2) = \operatorname{div}(h_1) - \operatorname{div}(h_2)$$

Principal divisors form a subgroup of the degree-zero divisors.

Divisor equivalence

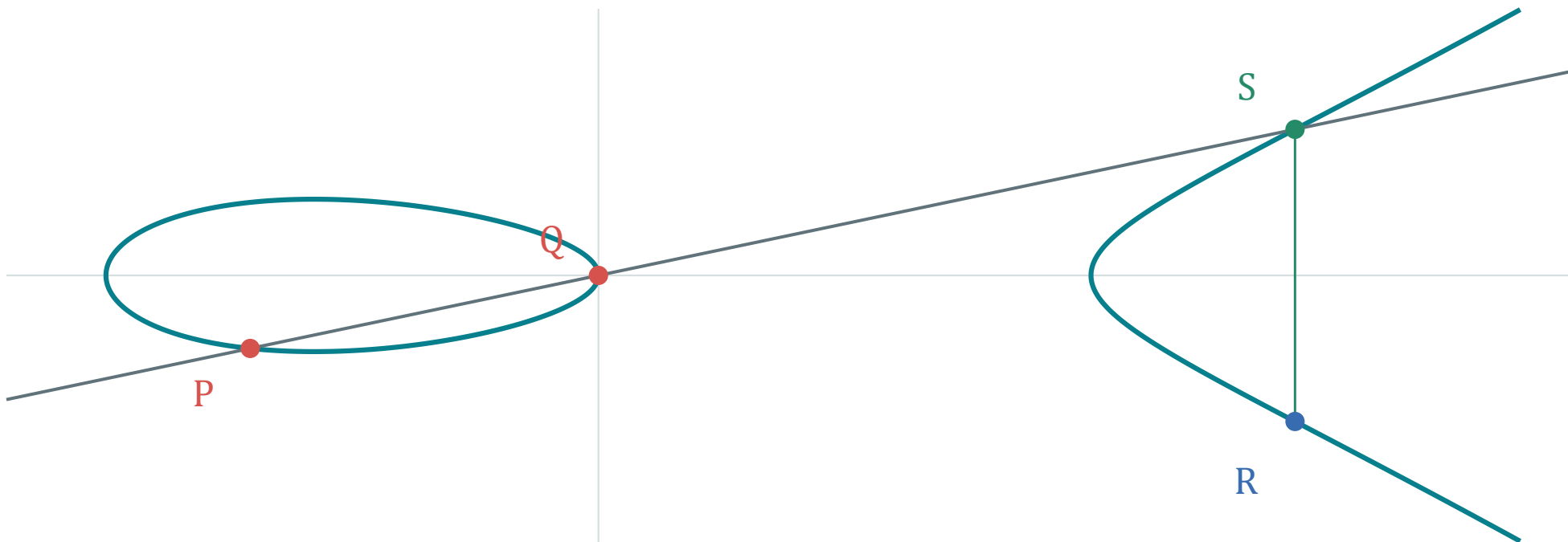


Two representatives of the same class

$$D \sim D' \iff D - D' = \text{div}(h)$$

A function gives a relation between two collections.

Reflection revisited



$$\operatorname{div}(v) = (S) + (R) - 2(\infty)$$

The vertical line pairs a point with its reflection.

Elliptic addition as an equivalence

The chord-and-tangent rule already uses divisor classes.

$$\operatorname{div}(\ell/v) = (P) + (Q) - (R) - (\infty)$$

$$(P) + (Q) - 2(\infty) \sim (R) - (\infty)$$

The Jacobian

$$J(C) = \text{Pic}^0(C) = \text{Div}^0(C) / \text{Prin}(C)$$

$$[D] + [E] = [D + E]$$

$$E \cong J(E), \quad P \mapsto [(P) - (\infty)]$$

Group elements are equivalence classes of degree-zero divisors.

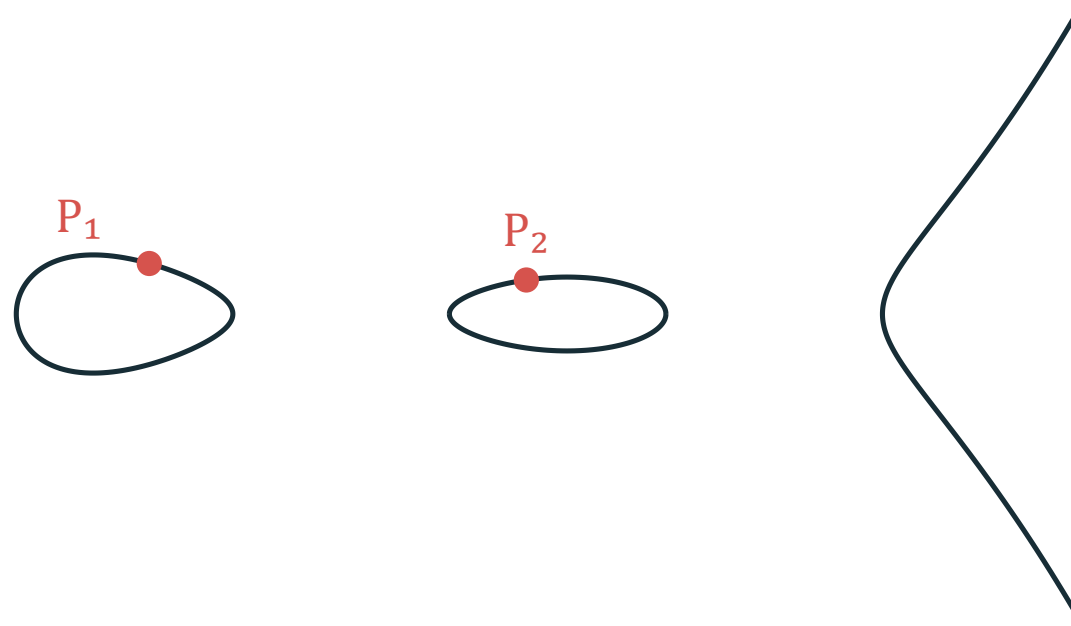
Reduced representatives

$$D_{\text{red}} = (P_1) + \cdots + (P_r) - r(\infty), \quad r \leq g$$

Every class has a unique reduced representative in our model.

Genus bounds the number of affine points needed.

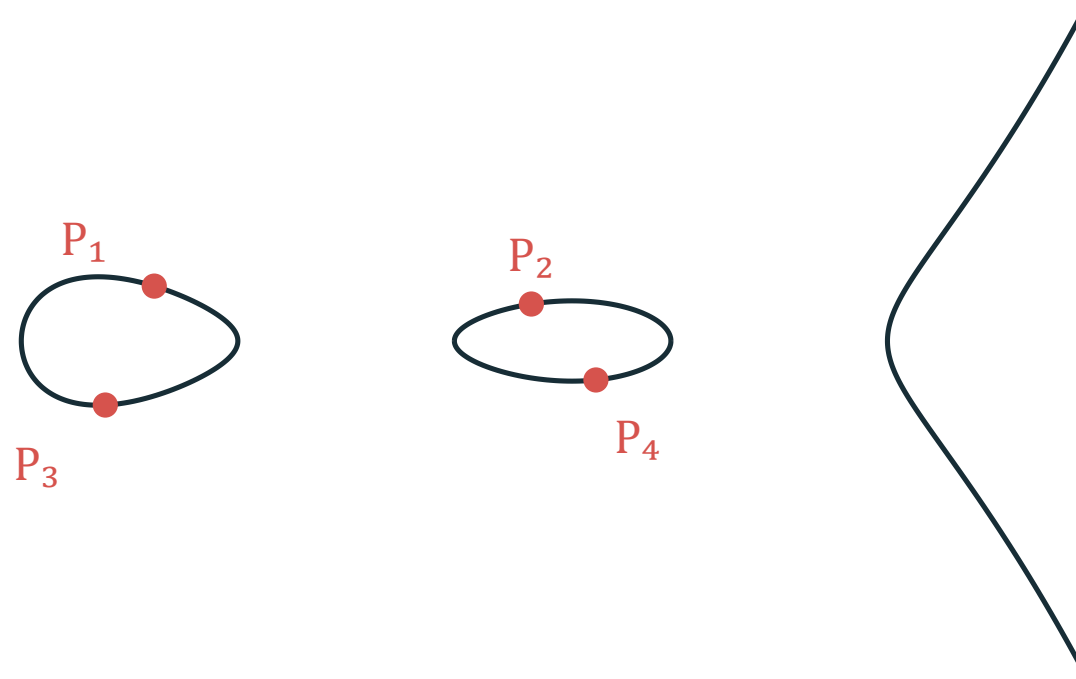
A genus-2 group element



$$D_1 = (P_1) + (P_2) - 2(\infty)$$

$$D_2 = (P_3) + (P_4) - 2(\infty)$$

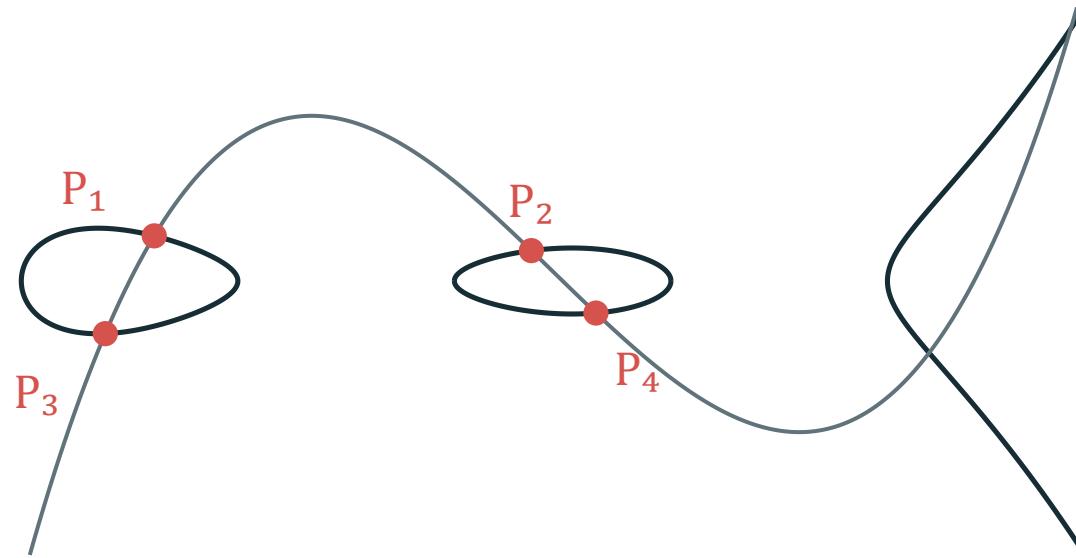
Addition produces four points



$$D = D_1 + D_2 = \sum_{i=1}^4 (P_i) - 4(\infty)$$

The sum has degree zero, but its representative needs reduction.

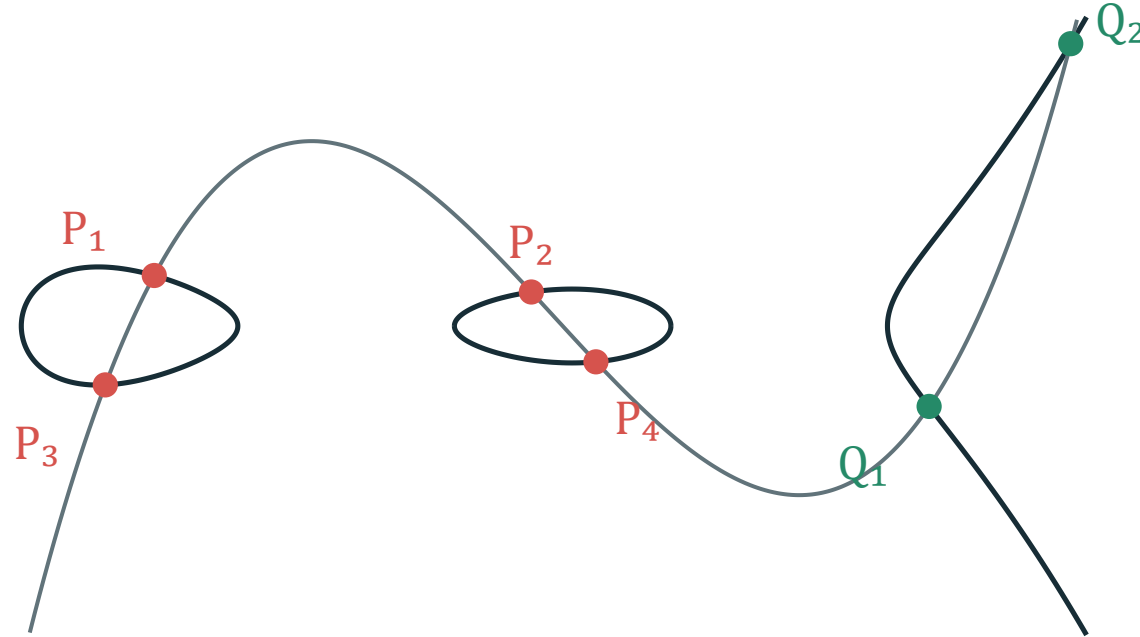
Cubic interpolation



$$v(x) = a_3x^3 + a_2x^2 + a_1x + a_0$$
$$f(x) - v(x)^2 = 0 \quad \text{has degree 6}$$

Four prescribed intersections leave two more.

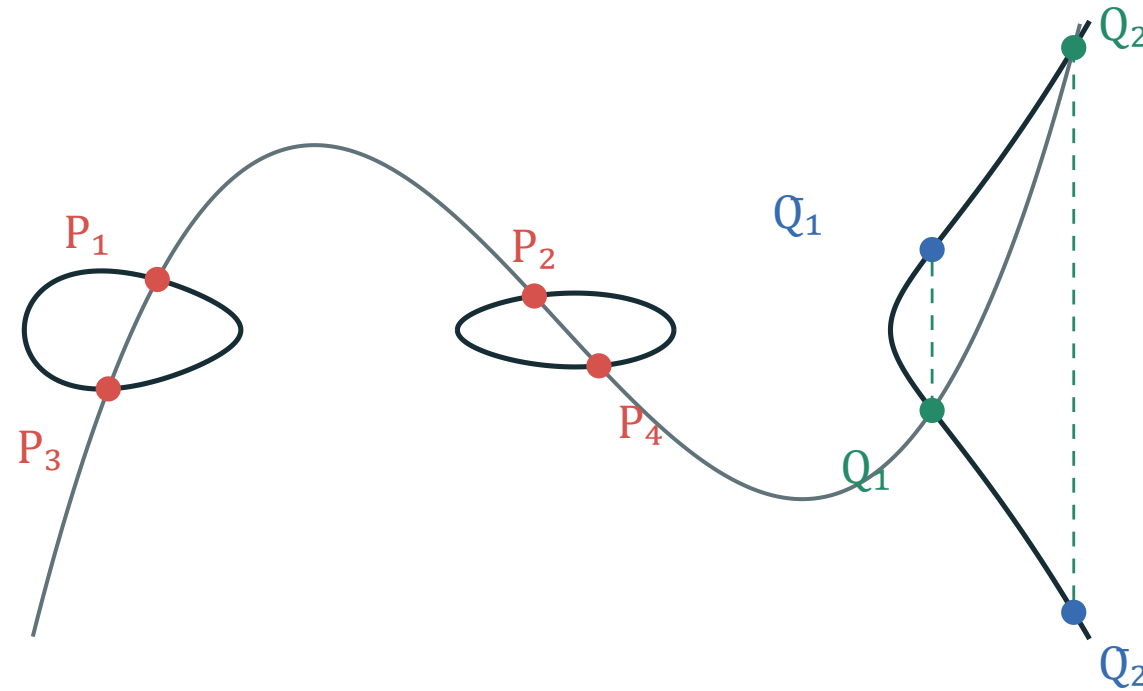
The remaining intersections



$$\operatorname{div}(\ell) = \sum_{i=1}^4 (P_i) + (Q_1) + (Q_2) - 6(\infty)$$

$$D \sim 2(\infty) - (Q_1) - (Q_2)$$

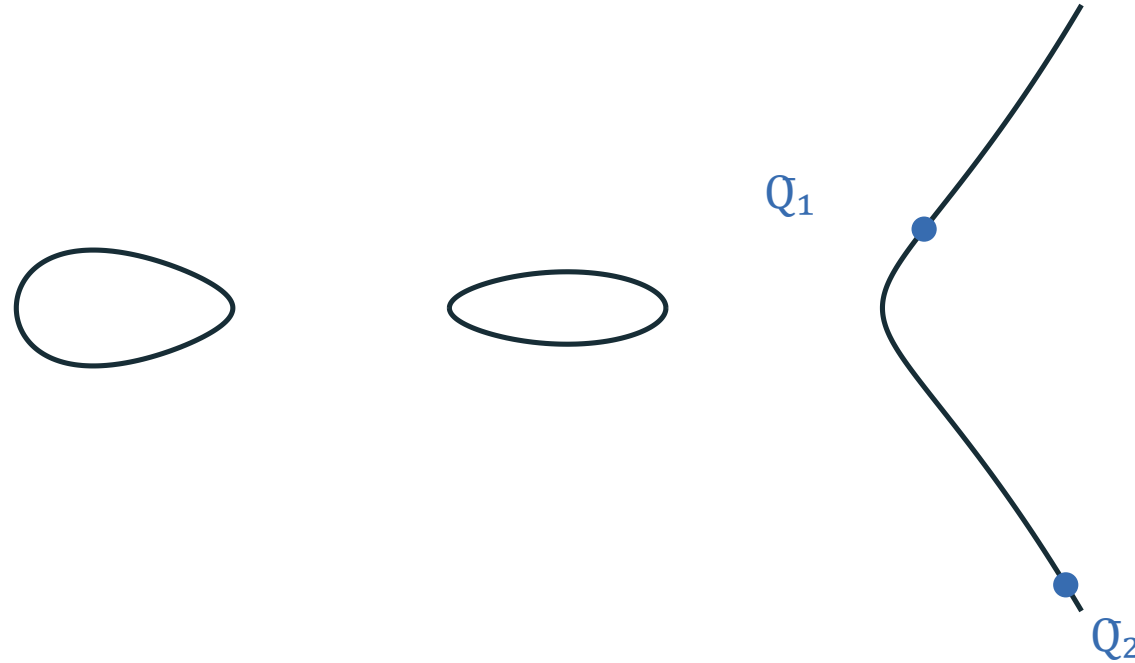
Reflection completes the reduction



$$\bar{Q} = (x_Q, -y_Q)$$

$$D \sim (\bar{Q}_1) + (\bar{Q}_2) - 2(\infty)$$

A closed addition law



$$[D_1] + [D_2] = [(\overline{Q_1}) + (\overline{Q_2}) - 2(\infty)]$$

Compose the input divisors.

Reduce using functions on the curve.

Mumford coordinates

A collection of points

$$P_1 = (x_1, y_1)$$

$$P_2 = (x_2, y_2)$$



A pair of polynomials

$$u = (x - x_1)(x - x_2)$$

$$v(x_i) = y_i$$

$$u(x) = \prod_i (x - x_i), \quad v(x_i) = y_i$$

$$u \mid (f - v^2), \quad \deg v < \deg u \leq g$$

Store the class as a pair of polynomials (u, v) .

A small example over $\mathbb{F}_{11}$

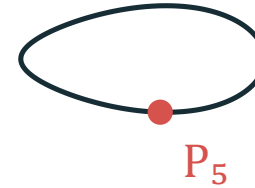
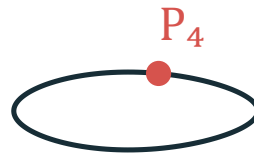
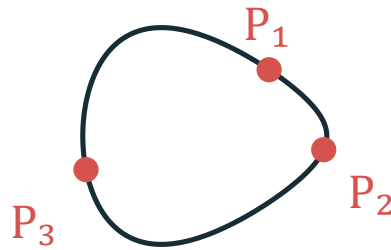
$$C/\mathbb{F}_{11}: y^2 = x^5 + x + 1$$

$$P = (0, 1), \quad Q = (1, 5)$$

$$(u, v) = (x^2 - x, 4x + 1)$$

The coefficients encode $[(P) + (Q) - 2(\infty)]$.

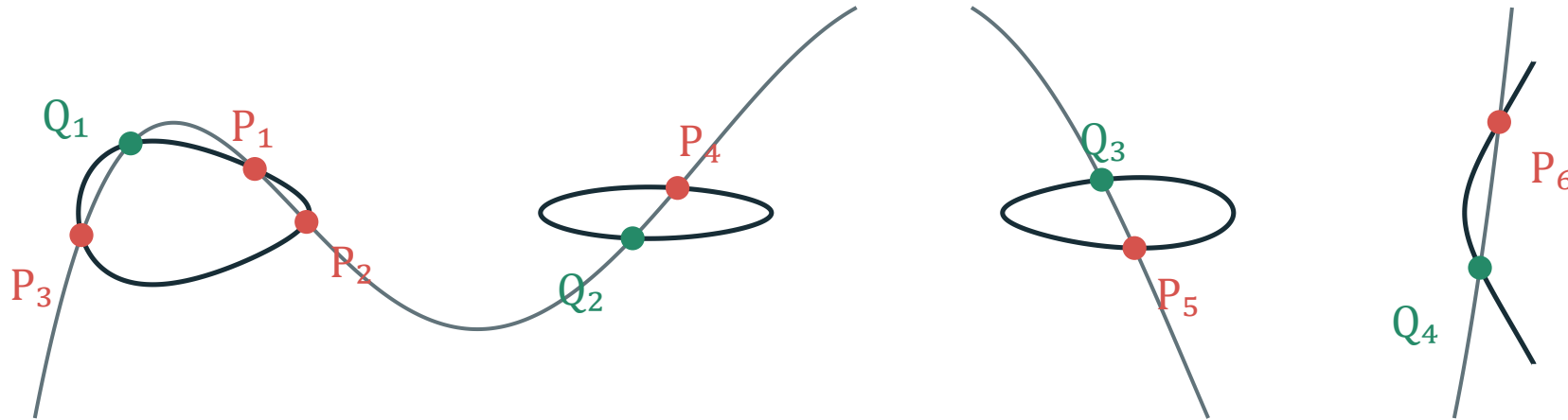
Genus 3 begins with six points



$$C: y^2 = f(x), \quad \deg f = 7$$

$$D = \sum_{i=1}^6 (P_i) - 6(\infty)$$

The first interpolator



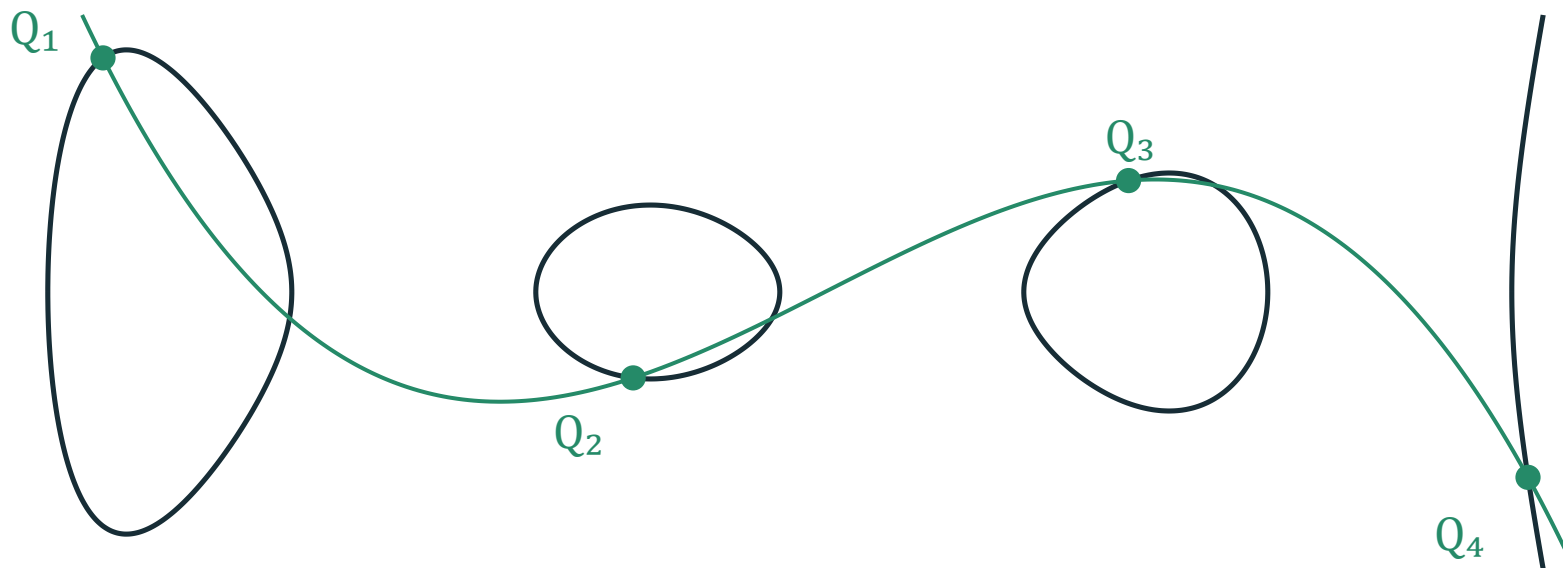
$$\deg v = 5, \quad \deg(f - v^2) = 10$$

$$A = \sum_{j=1}^4 (Q_j) - 4(\infty)$$

$$D + A \sim 0$$

Six known intersections leave four new ones.

Four points still need reduction



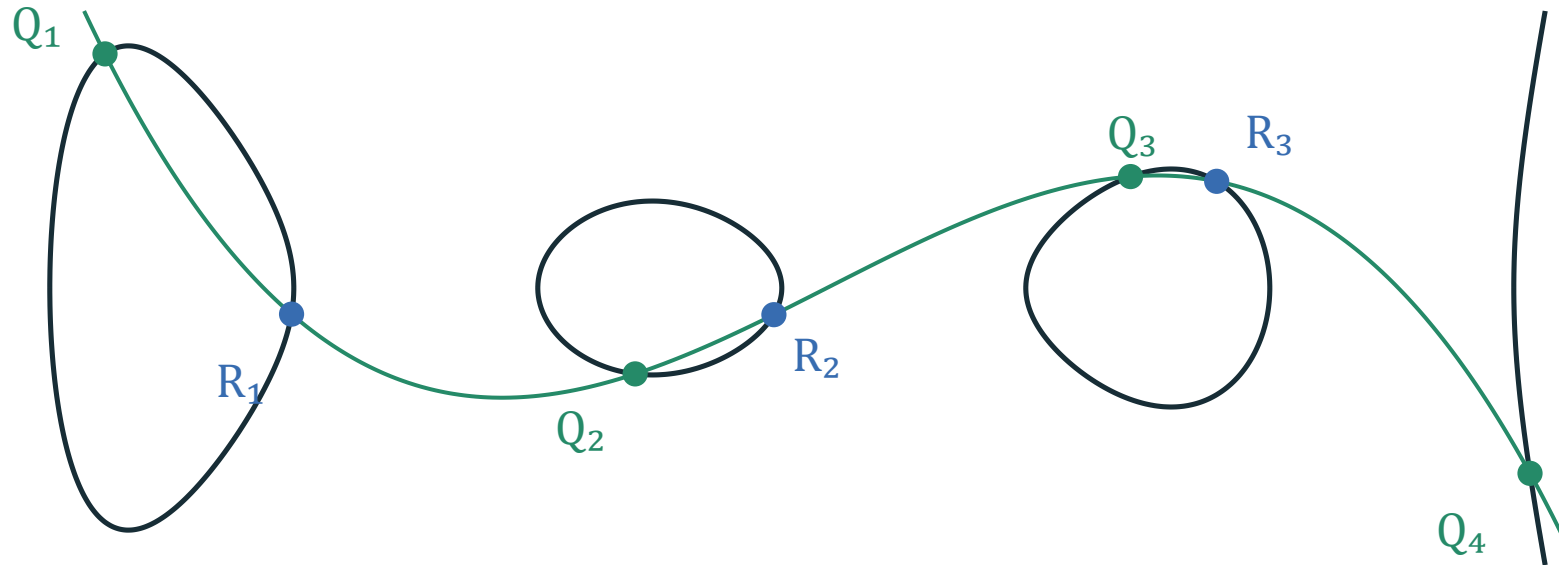
Vertical scale enlarged

$$\deg w = 3, \quad \deg(f - w^2) = 7$$

$$A + D' \sim 0$$

A cubic through four points leaves three more.

Three points represent the answer



Vertical scale enlarged

$$D + A \sim 0, \quad A + D' \sim 0$$
$$D \sim D' = \sum_{k=1}^3 (R_k) - 3(\infty)$$

Two sign changes return to the original class.

Polynomial arithmetic computes the group law

$$[n]G = G + \cdots + G$$

Mumford coordinates store reduced classes.

Cantor's algorithm composes and reduces them.

Repeated additions and doublings compute scalar multiples.

Diffie–Hellman in the Jacobian

Alice

Public generator G of prime order

Bob

a

b

$[a]G$

$[b]G$

$[ab]G$

shared element

$[ab]G$

$$G \in J(C)(\mathbb{F}_q), \quad \text{ord}(G) = r \text{ prime}$$

$$A = [a]G, \quad B = [b]G, \quad S = [ab]G$$

Genus changes the security calculation

$$\#J(C)(\mathbb{F}_q) \approx q^g$$

A larger Jacobian can use a smaller base field.

Arithmetic costs and available attacks both change.

Security depends on the subgroup and the curve family.

The Jacobian has dimension g

1

dimension

Elliptic curve

$$J(E) \cong E$$

2

dimension

Abelian surface

$$J(C_2)$$

3

dimension

Abelian threefold

$$J(C_3)$$

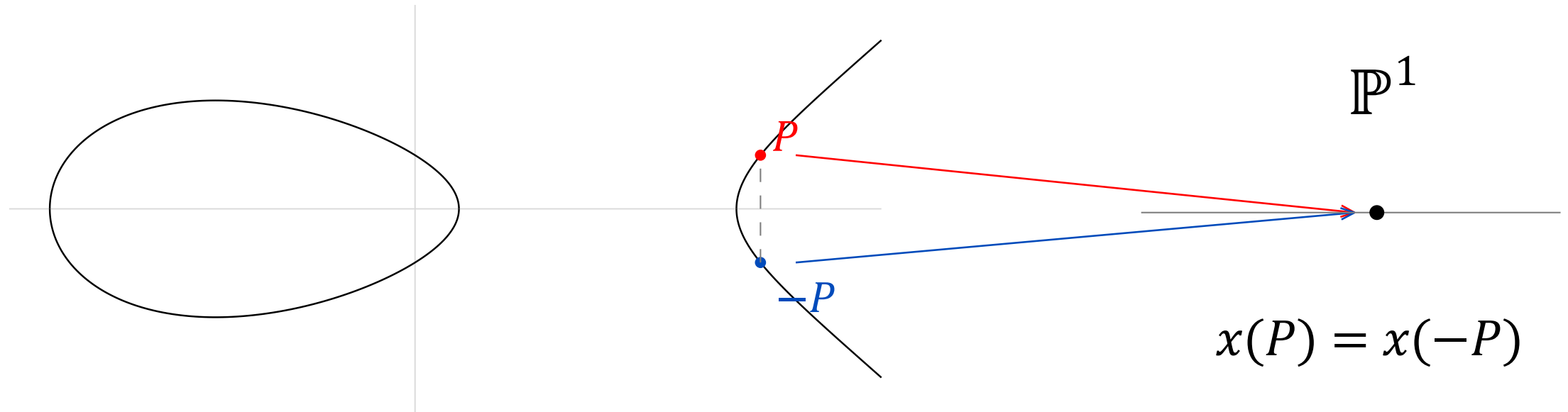
$$\dim C = 1, \quad \dim J(C) = g$$

Genus 2 gives an abelian surface.

Genus 3 gives an abelian threefold.

Elliptic curves: forgetting the sign

On an elliptic curve, P and $-P$ have the same x -coordinate.



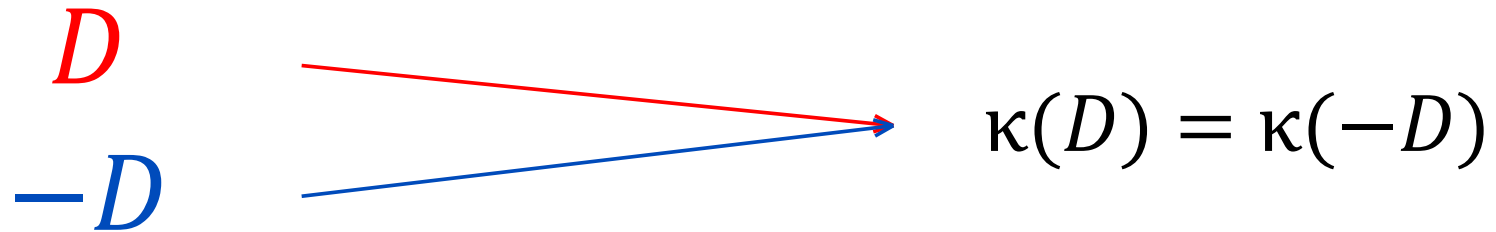
$$E/\{\pm 1\} \cong \mathbb{P}^1$$

Scalar multiplication still makes sense after forgetting the sign.

Forget the sign of a divisor class

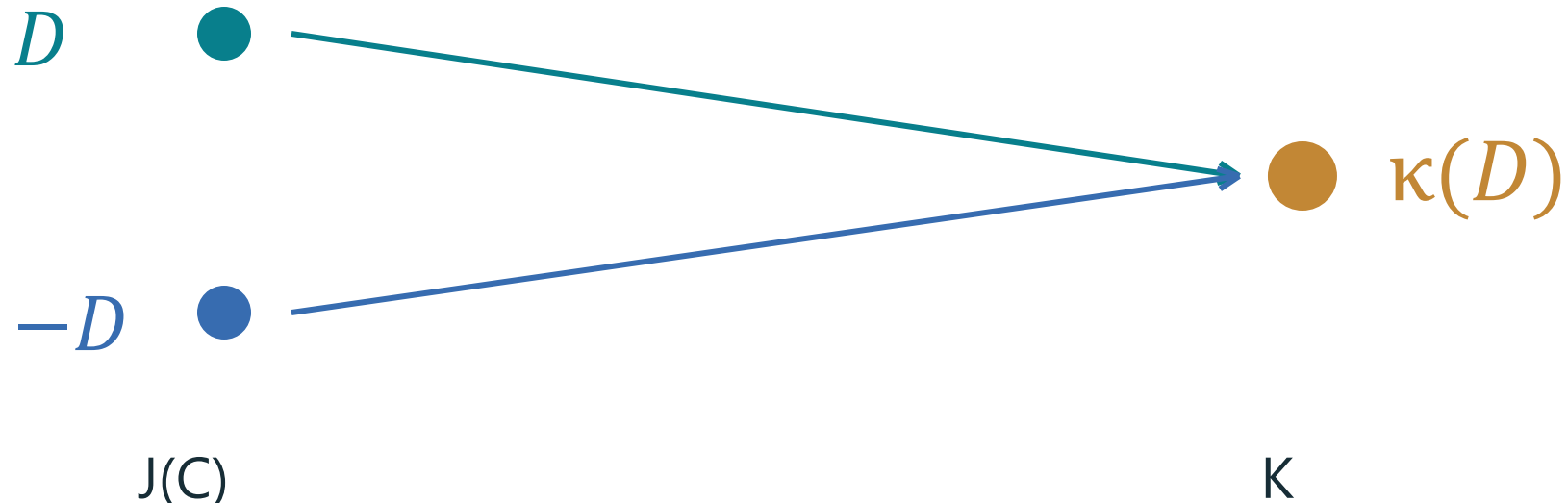
The same idea works for the genus-2 Jacobian.

$$\kappa: J \longrightarrow K = J/\{\pm 1\}$$


$$\begin{array}{c} D \\ -D \end{array} \quad \begin{array}{c} \text{red arrow} \\ \text{blue arrow} \end{array} \quad \kappa(D) = \kappa(-D)$$

$$(u, v) \sim (u, -v)$$

Forgetting the sign

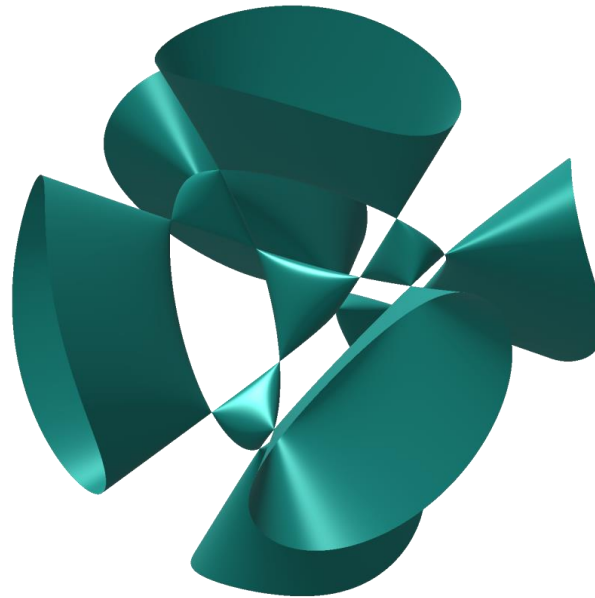


$$\kappa(D) = \kappa(-D)$$

$$K = J(C)/\{\pm 1\}$$

Elliptic x-coordinates already forget the sign.

A Kummer surface



A real-locus illustration

$$\dim J(C) = 2 \implies K \text{ is a surface}$$

A quartic model in projective 3-space.

A real rendering shows one view of the algebraic surface.

Two projective models

$$J[2](\bar{k}) \cong (\mathbb{Z}/2\mathbb{Z})^4 \quad (\text{char } k \neq 2)$$

	Jacobian	Kummer
Standard construction	 40 	 20
Projective space	$\mathbb{P}^{15}$	$\mathbb{P}^3$
Homogeneous coordinates	16	4
Defining equations	72 quadrics	1 quartic
Dimension	2	2

The 16 fixed points of negation become 16 nodes.

Gaudry's fast Kummer coordinates

Use four homogeneous coordinates $(X:Y:Z:T)$.

A squared-theta model is a single quartic:

$$Q = X^2 + Y^2 + Z^2 + T^2 - F(XT + YZ) \\ - G(XZ + YT) - H(XY + ZT)$$

$$Q^2 = \varepsilon XYZT$$

Enough arithmetic for scalar multiplication

$$\kappa(D) \mapsto \kappa(2D)$$

$$\kappa(D), \kappa(E), \kappa(D - E) \mapsto \kappa(D + E)$$

Doubling and differential addition support a Montgomery ladder.

Field and subgroup sizes

For this example, $\#J(\mathbb{F}_p) = 16r$ with a 250-bit prime r .

Gaudry–Schost: $p = 2^{127} - 1$.

$$\#E(\mathbb{F}_q) \approx q, \quad \#J(\mathbb{F}_p) \approx p^2$$

	Curve25519	Gaudry–Schost
Field size	255 bits	127 bits
Prime subgroup	$\approx 2^{252}$	$\approx 2^{250}$
Generic square-root exponent	≈ 126	≈ 125

Comparable sizes; actual subgroup exponents are shown.

Higher-dimensional Kummer varieties

1

dimension

Kummer line

$$E / \{\pm 1\}$$

2

dimension

Kummer surface

$$J(C_2) / \{\pm 1\}$$

3

dimension

Kummer threefold

$$J(C_3) / \{\pm 1\}$$

$$\dim(J(C)/\{\pm 1\}) = g$$

Genus 3 gives a Kummer threefold.

Explicit models extend beyond what a single picture can show.

Geometry can change the representation

$$\kappa: J(C) \longrightarrow K$$

Jacobian points retain the sign.

Kummer arithmetic can accelerate scalar multiplication.

Suitable recovery algorithms return the signed output.

The group behind the curve

The cryptographic group is the Jacobian.

Divisors describe its elements.

Functions explain the relations.

Reduction makes the arithmetic finite and concrete.

Questions?