Pairings, index calculus, and hyperelliptic curves

Tanja Lange
Technische Universiteit Eindhoven

with some slides by
Daniel J. Bernstein

Pairings

Let $(G_1, +), (G_1', +)$ and $(G_T, \cdot)$ be groups of prime order ℓ and let

$e : G_1 \times G_1' \to G_T$

be a map satisfying

$e(P + Q, R') = e(P, R')e(Q, R'),$

$e(P, R' + S') = e(P, R')e(P, S').$

Request further that e is non-degenerate in the first argument, i.e., if for some P $e(P, R') = 1$ for all $R' \in G_1'$, then P is the identity in G_1

Such an e is called a *bilinear map* or *pairing*.

Consequences of pairings

Assume that $G_1 = G_1'$,
in particular $e(P, P) \neq 1$.

Then for all triples
$(aP, bP, cP) \in \langle P \rangle^3$
one can decide in time
polynomial in $\log \ell$ whether
$c = \log_P(cP) = \log_P(aP) \log_P(bP) = ab$
by comparing
$e(aP, bP) = e(P, P)^{ab}$ and
$e(P, cP) = e(P, P)^c$.

This means that the decisional
Diffie-Hellman problem is easy.

The DL system G_1 is at most as secure as the system G_T.

Even if $G_1 \neq G_1'$ one can
transfer the DLP in G_1
to a DLP in G_T,
provided one can find an element
$P' \in G_1'$ such that the map
$P \to e(P, P')$ is injective.
This is easy
if G_1' can be sampled.

Pairings are interesting attack tool if DLP in G_T is easier to solve; e.g. if G_T has index calculus attacks.

Pairing based protocols I

Joux, ANTS 2000,

one round tripartite key exchange

Let P, P' be generators of G_1 and G_1' respectively.

Users A, B and C compute joint secret from their secret contributions a, b, c as follows (A's perspective):

- Compute and send aP, aP'.
- Upon receipt of bP and cP' put $k = (e(bP, cP'))^a$.

The resulting element k is the same for each participant as

$$\begin{aligned} k &= (e(bP, cP'))^a \\ &= (e(P, P'))^{abc} \\ &= (e(aP, cP'))^b \\ &= (e(aP, bP'))^c. \end{aligned}$$

- Obvious saving in first step if $G_1 = G_1'$.
- Only one user needs to do computations in G_1 and G_1'.

Pairing based protocols II

Boneh and Franklin, Crypto 2001,
ID-based cryptography
(earlier proposal by Sakai-Ohgishi-Kasahara in 2000 using pairings)

Consequences

- Recipient need not have a public key;
- Setup requires trusted authority, TA can compute any secret key.

Let $H : \{0,1\}^* \to G_1'$ be hash function.

Master secret key of TA is s, public key is $P_{pub} = sP$.

Encryption:

- Compute $H(ID) \in G_1'$.
- Choose random nonce k, compute $R = kP$.
- Compute $c = (e(P_{pub}, H(ID)))^k \oplus m$ and send (R, c).

Decryption:

- Obtain secret key $S' = sH(ID) \in G_1'$ from TA.
- Compute $c \oplus e(R, S') = m$.

$$
\begin{aligned}
e(R, S') &= e(kP, sH(ID)) \\
&= (e(P, H(ID)))^{ks} \\
&= (e(sP, H(ID)))^k \\
&= (e(P_{pub}, H(ID)))^k
\end{aligned}
$$

Security assumptions

Clearly these systems require hard DLPs in G_1, G_1', G_T.

New assumptions:

Computational Bilinear Diffie-Hellman Problem (CBDHP):

Compute $abcP$

given aP, bP, cP and P

Decisional Bilinear Diffie-Hellman Problem (DBDHP):

Given P, aP, bP, cP and rP

decide whether $rP = abcP$.

We want to define pairings
$G_1 \times G_1' \to G_T$
preserving the group structure.

The pairings map from
an elliptic curve $G_1 \subset E/\mathbf{F}_q$
to the multiplicative group of a
finite extension field $\mathbf{F}_{q^k}$.

To embed the points of order ℓ
into $\mathbf{F}_{q^k}$ there need to be ℓ-th
roots of unity are in $\mathbf{F}_{q^k}^*$.

The *embedding degree* k satisfies
k is minimal with $\ell \mid q^k - 1$.

E is supersingular if
$E[p^s](\overline{\mathbf{F}}_q) = \{\infty\}$.
$t \equiv 0 \bmod p$.
Endomorphism ring of E
is order in quaternion algebra.

Otherwise it is ordinary and one
has $E[p^s](\overline{\mathbf{F}}_q) = \mathbf{Z}/p^s\mathbf{Z}$.
These statements hold for all s if
they hold for one.

Example:
$y^2 + y = x^3 + a_4x + a_6$ over $\mathbf{F}_{2^r}$
is supersingular, as a point of
order 2 would satisfy $y_P = y_P + 1$
which is impossible.

Embedding degrees

Let $E/\mathbf{F}_p$ be supersingular and $p \geq 5$, i.e $p > 2\sqrt{p}$.

Hasse's Theorem states
$|t| \leq 2\sqrt{p}$.
E supersingular implies
$t \equiv 0 \bmod p$, so $t = 0$ and
$|E(\mathbf{F}_p)| = p + 1$.

Obviously
$(p+1) \mid (p^2 - 1) = (p+1)(p-1)$
so $k \leq 2$ for supersingular curves over prime fields.

Distortion maps

For supersingular curves there exist homomorphisms
$\phi : E(\mathbf{F}_q) \to E(\mathbf{F}_{q^k})$
so that $e(P, \phi(P)) = \tilde{e}(P, P) \neq 1$
for $P \neq \infty$.
Such a map is called a *distortion map*.

These maps are convenient for protocol design because they give a pairing
$\tilde{e} : G_1 \times G_1 \to G_T$
for $\tilde{e}(P, P) = e(P, \phi(P))$.

Examples:

1. $y^2 = x^3 + x$,

for $p \equiv 3 \pmod 4$.

Distortion map

$(x, y) \mapsto (-x, \sqrt{-1}y)$.

2. $y^2 = x^3 + a_6$,

for $p \equiv 2 \pmod 3$.

Distortion map $(x, y) \mapsto (\zeta_3 x, y)$

with $\zeta_3^3 = 1, \zeta_3 \neq 1$.

In both cases,

$\#E(\mathbf{F}_p) = p + 1$.

$p = 1000003 \equiv 3 \bmod 4$ and
$y^2 = x^3 - x$ over $\mathbf{F}_p$.
Has $1000004 = p + 1$ points.
$P = (101384, 614510)$ is a point
of order 500002.
$nP = (670366, 740819)$.
Construct $\mathbf{F}_{p^2}$ as $\mathbf{F}_p(i)$.
$\phi(P) = (898619, 614510i)$.

Invoke computer algebra and
compute
$e(P, \phi(P)) = 387265 + 276048i$;
$e(Q, \phi(P)) = 609466 + 807033i$.
Solve DLP in $\mathbf{F}_p(i)$
to get $n = 78654$.
(This is the clock from Monday).

Summary of pairings

Menezes, Okamoto, and Vanstone for E supersingular:
For $p = 2$ have $k \leq 4$.
For $p = 3$ we $k \leq 6$
Over $\mathbf{F}_p$, $p \geq 5$ have $k \leq 2$.
These bounds are attained.

Not only supersingular curves:
MNT curves are non-supersingular curves with small k.
Other examples constructed for pairing-based cryptography –
but small k unlikely to occur for random curve.

Index calculus in prime fields

Index calculus is a method to compute discrete logarithms. Works in many situations but depends on group (not generic attack)

p prime, elements of $\mathbf{F}_p$ represented by numbers in $\{0, 1, \ldots, p-1\}$;
g generator of multiplicative group.

If $h \in \mathbf{F}_p$ factors as
$h = h_1 \cdot h_2 \cdots h_n$ then

$$h = g^{a_1} \cdot g^{a_2} \cdots g^{a_n}$$
$$= g^{a_1 + a_2 + \ldots + a_n},$$

with $h_i = g^{a_i}$.

Knowledge of the a_i,
i.e., of the discrete logarithms of
h_i to base g,
gives knowledge of the discrete
logarithm of h to base g.

If h factors appropriately . . .

If h factors appropriately?!

Ensure by finding h' with known DL s.t. $h \cdot h'$ factors over the h_i. So far: instead of finding *one* DL we have to find *many* DLs *and* they have to fit to h *and* we have to find a suitable h' *and* factor numbers.

Two different settings –
the integers modulo p and
the integers themselves.
Factorization takes place over **Z**, while the left hand side is reduced modulo p.

Select $F = \{g_1, g_2, \ldots, g_m\}$
so that $\bar{h} < p$ is likely to factor
into powers of g_i.
F called *factor base*.

An equation of form
$\bar{h} = g_1^{n_1} \cdot g_2^{n_2} \cdots g_m^{n_m}$,
with $n_i \in \mathbf{Z}$ is called a *relation*.
Choose F as small primes , e.g.
$g_1 = 2, g_2 = 3, g_3 = 5, \ldots$

Generate many relations with
known DL of $\tilde{h}_j = g^{k_j}$
$\tilde{h}_j = g^{k_j} = g_1^{n_{j1}} \cdot g_2^{n_{j2}} \cdots g_m^{n_{jm}}$.
(This means discarding
g^{k_j} if it does not factor .)

Matrix of relations

For each relation
$\tilde{h}_j = g^{k_j} = g_1^{n_{j1}} \cdot g_2^{n_{j2}} \cdots g_m^{n_{jm}}$

enter the row

$$(n_{j1} n_{j2} \ldots n_{jm} | k_j)$$

into a matrix $M =$

$$\begin{pmatrix} n_{11} & \ldots & n_{1i} & \ldots & n_{m1} & k_1 \\ n_{21} & \ldots & n_{2i} & \ldots & n_{m2} & k_2 \\ \vdots & & \vdots & & \vdots & \vdots \\ n_{l1} & \ldots & n_{li} & \ldots & n_{lm} & k_l \end{pmatrix}$$

The i-th column

corresponds to the unknown a_i

so that $g_i = g^{a_i}$.

Computing DLPs

Use linear algebra to solve for a_is.
This step does not depend on the target DLP $h = g^a$.
A single relation $h \cdot g^k$ factoring over F gives the DLP.

Running time (with much more clever way of finding relations) $O(\exp(c \log p^{1/3} \log(\log p)^{2/3}))$ for some c.
This is subexponential in $\log p$!
Notation: write this complexity as $L(1/3, c)$.

Similar for $\mathbf{F}_{2^n}$

Elements of $\mathbf{F}_{2^n}$ are represented as $\mathbf{F}_{2^n} = \{\sum_{i=0}^{n-1} c_i x^i | c_i \in \mathbf{F}_2, 0 \le i < n\}$, i.e. polynomials of degree less than n modulo an irreducible polynomial $f(x) \in \mathbf{F}_2[x]$.

Factoring into powers of small primes is replaced by factoring into irreducible polynomials of small degree.

Same approach works for all finite fields $\mathbf{F}_{p^n}$ in $O(\exp(c' \log p^{1/3} \log(\log p)^{2/3}))$.
Smaller p have smaller constant c.

Same approach works for all finite fields $\mathbf{F}_{p^n}$ in $O(\exp(c' \log p^{1/3} \log(\log p)^{2/3}))$.
Smaller p have smaller constant c.

If DLP in $\mathbf{F}_{q^k}^*$ is weak can break pairing system in target group $G_T \subset \mathbf{F}_{q^k}^*$.
Big computation in 2011: Hayashi, Shinohara, Shimoyama, and Takagi solved DLP in $\mathbf{F}_{3^{6\cdot 97}}^*$
This field was considered as target field for pairings over supersingular curves $E/\mathbf{F}_{3^{97}}$ with embedding degree 6.

More recent development

Flurry of papers with breathtaking improvements and new records by Joux and by Göloglu, Granger, McGuire, and Zumbrägel (GGMZ)

Joux 2012-12-24, 1175-bit and 1425-bit

Joux 2013-02-11 $\mathbf{F}^*_{2^{1778}}$

GGMZ 2013-02-19 $\mathbf{F}^*_{2^{1971}}$

Joux 2013-03-22 $\mathbf{F}^*_{2^{4080}}$

GGMZ 2013-04-11 $\mathbf{F}^*_{2^{6120}}$

Joux 2013-05-21 $\mathbf{F}^*_{2^{6168}}$

$\vdots$

Theoretical results

Barbulescu, Gaudry, Joux, Thomé
2013-06-18
Quasi-polynomial time algorithm
to compute DLs in $\mathbf{F}_{p^n}^*$.
Strongly depends on p, so only
efficient for small p.
Best speeds for composite n.

Also interesting
Joux 2013-02-20 $L(1/4 + o(1), c)$

Hyperelliptic curves

Affine equation of hyperelliptic curve of genus g (with $\mathbf{F}_q$-rational Weierstraß-point at infinity)

$C : y^2 + h(x)y = f(x)$.

$h(x), f(x) \in \mathbf{F}_q[x]$, f monic,

$\deg f = 2g + 1, \deg h \leq g$

C non singular:

No $(a, b) \in C(\overline{\mathbf{F}_q})$ satisfies

$2b + h(a) = 0$ and

$h'(a)b - f'(a) = 0$.

Examples

Concerning the arithmetic properties one can consider elliptic curves as hyperelliptic curves, i.e.

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$$

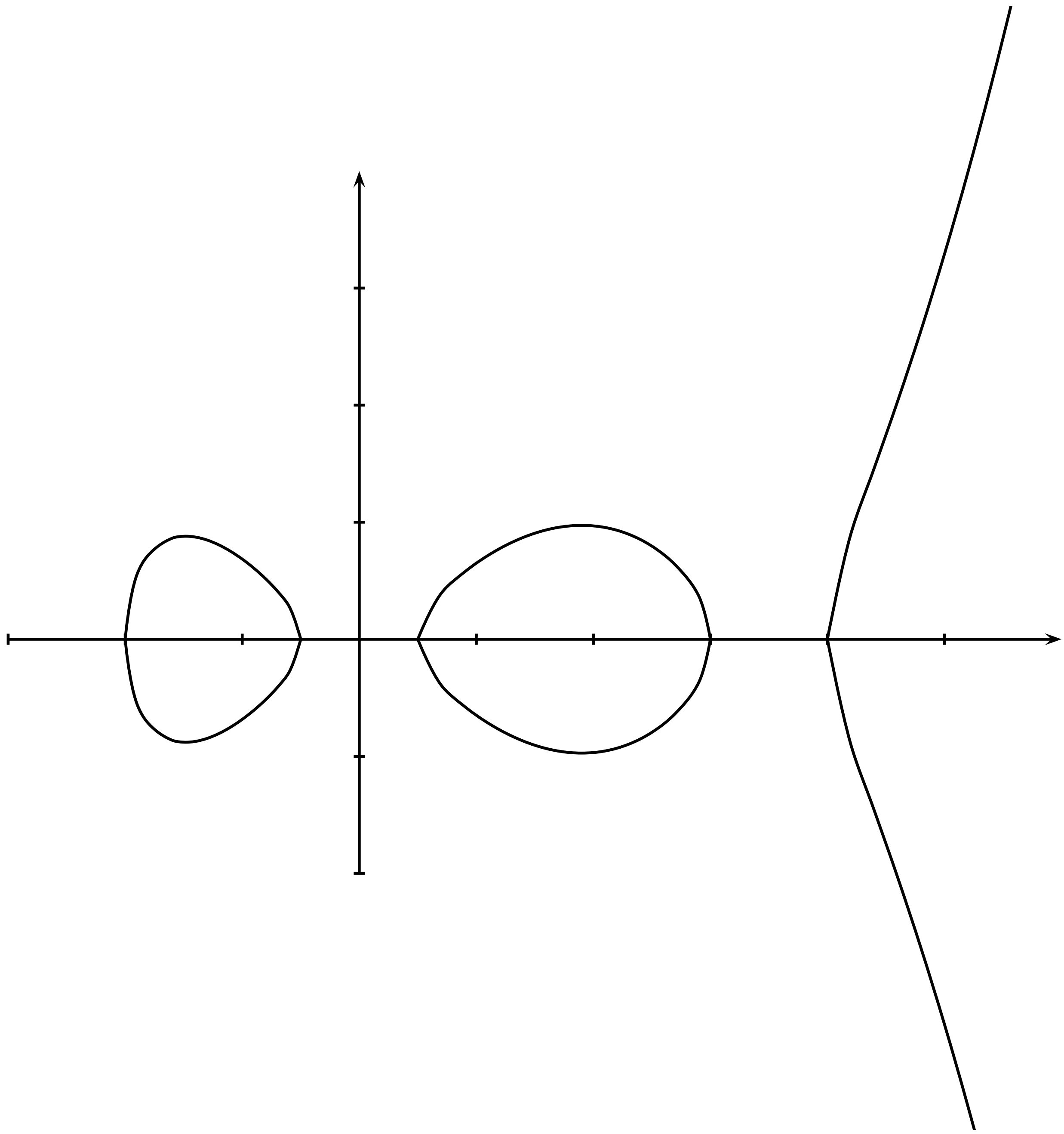
is considered as curve of genus 1.

Curve of genus 2 over field of odd characteristic

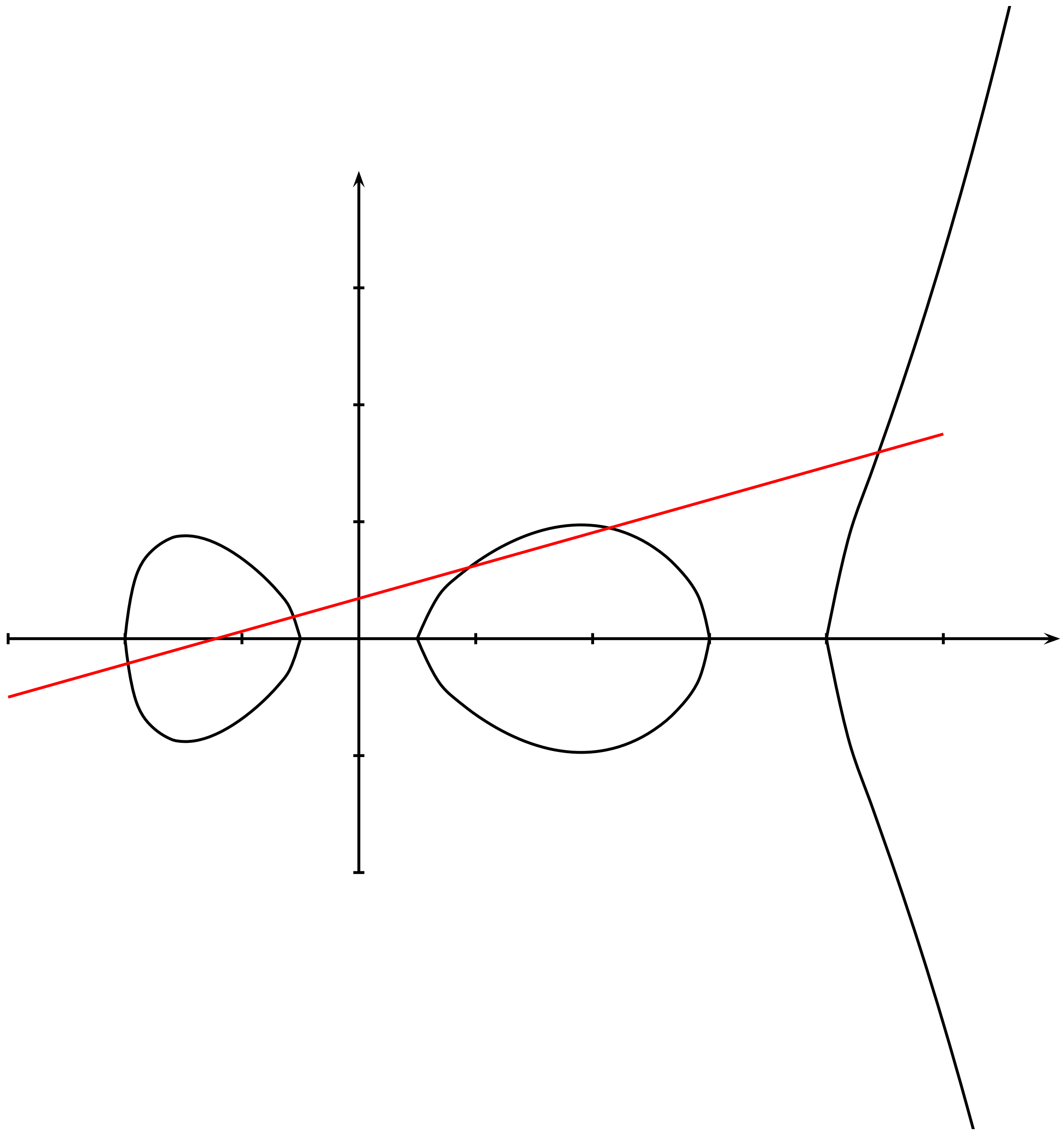
$$y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

provided $f(x)$ has no multiple roots.

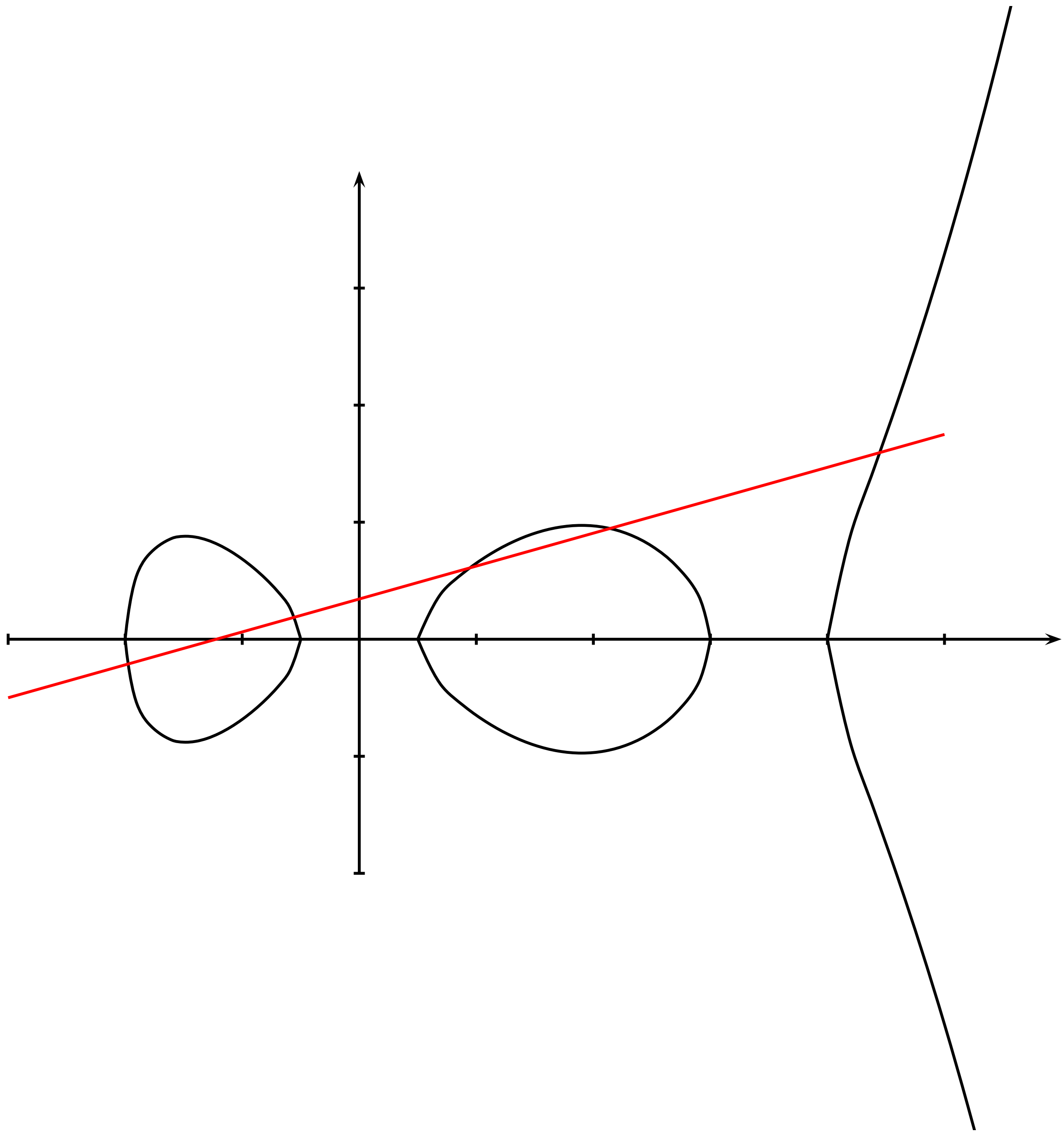
Curve of genus 2 over $\mathbf{R}$, $h = 0$



Curve of genus 2 over $\mathbf{R}$, $h = 0$



Curve of genus 2 over $\mathbf{R}$, $h = 0$



Points do **not** form a group!

Group of Divisors

Construct group from points on curve. Free abelian groups are in particular groups, and so associativity etc. follow immediately.

Construction uses Divisors, i.e. finite sums of points (elements of free abelian group),

$\sum_{P \in C(\overline{\mathbf{F}_q})} n_P P,\ n_P \in \mathbf{Z}$
with $n_P = 0$ for almost all P.

Addition works component-wise:

$(P_1 + 2P_2 - P_3) + (P_1 + P_2 + P_4)$
$= 2P_1 + 3P_2 - P_3 + P_4.$

Divisors

Effective divisors are divisors $D = \sum_{P \in C(\overline{\mathbf{F}_q})} n_P P$, $n_P \in \mathbf{Z}$ for which each $n_P \geq 0$.

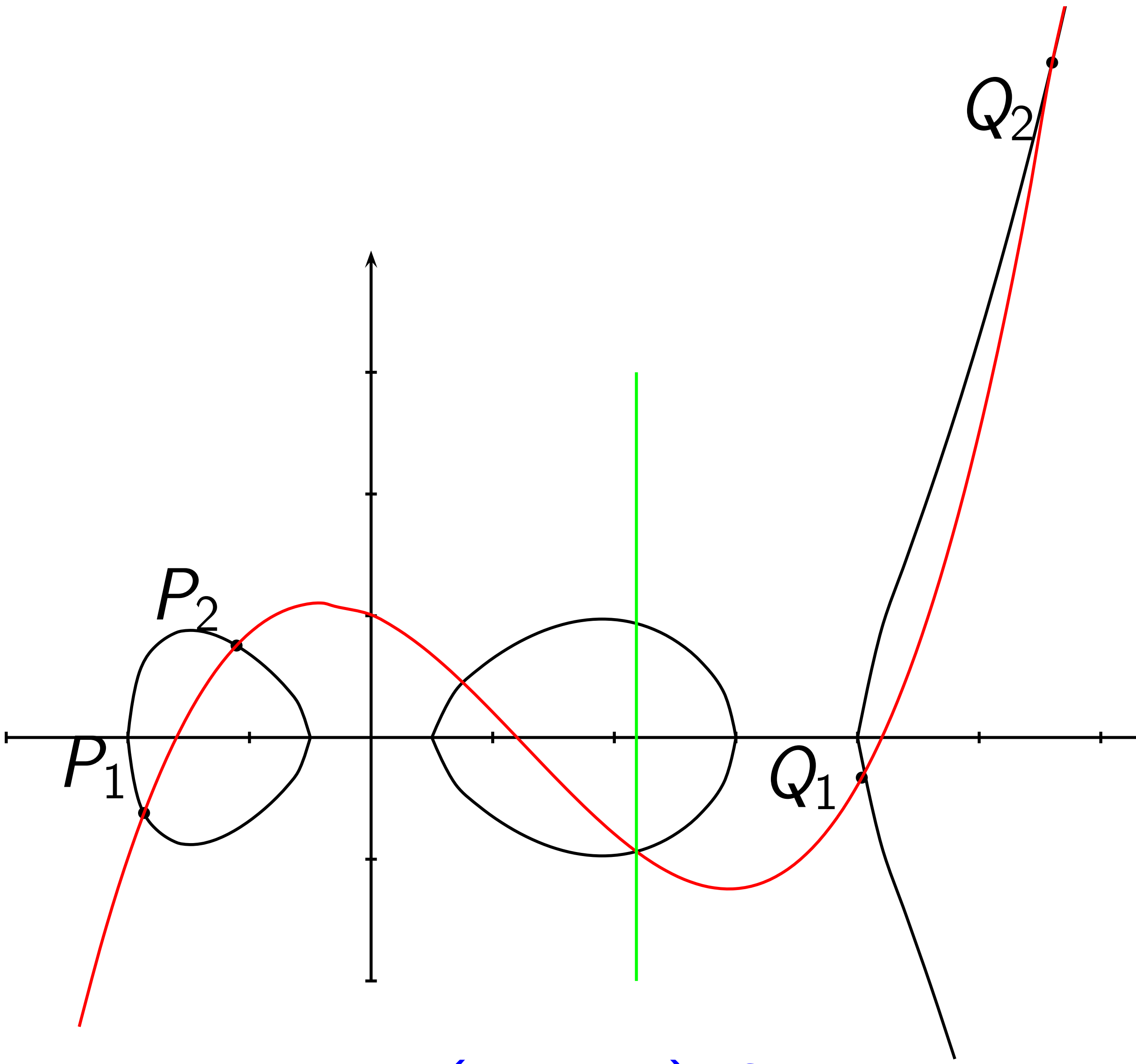
The degree of a divisor is $\deg(D) = \sum_{P \in C(\overline{\mathbf{F}_q})} n_P$.
$\deg(P_1 + 2P_2 - P_3) = 1 + 2 - 1 = 2$, $\deg(P_1 + P_2 + P_4) = 3$, $\deg(2P_1 + 3P_2 - P_3 + P_4) = 5$.

Divisors of degree zero form a group Div_C^0 with component-wise addition.

Principal divisors

Graph $F(x, y) = 0$ intersects curve in some points of $C(\overline{\mathbf{F}_q})$. Let v_P be normalized valuation $P \in C(\overline{\mathbf{F}_q})$, thus $v_P(F) = n \geq 0$ iff F has intersection of multiplicity n with curve at P (simple intersection has $n = 1$; tangent has $n \geq 2$).
Negative value = pole multiplicity.
Associate divisor to $F \in \mathbf{F}_q(C)$: $\mathrm{div}(F) = \sum_{P \in C(\overline{\mathbf{F}_q})} v_P(F) P$.
Such divisors are called principal divisors Princ_C. One can show that they have degree zero.

Curve of genus 2 over $\mathbf{R}$, $h = 0$



Points on red line (-6∞) form principal divisor

Points on green line (-2∞) form principal divisor

Here only $F(x, y) = y - k(x)$.

Divisor class group

Factor group of degree zero divisors Div_C^0 modulo principal divisors.
Constructs divisor class group of degree zero: $\mathrm{Pic}_C^0 = \mathrm{Div}_C^0/\mathrm{Princ}_C$.

So far working over $\overline{\mathbf{F}_q}$.
First definition:
$\mathbf{F}_q$-rational elements $\mathrm{Pic}_C^0(\mathbf{F}_q)$ remain fixed under Frobenius, i.e. q-th powers of all coordinates.
Not each point needs to remain fixed for that (sum can be rearranged).

Representation – elliptic curves

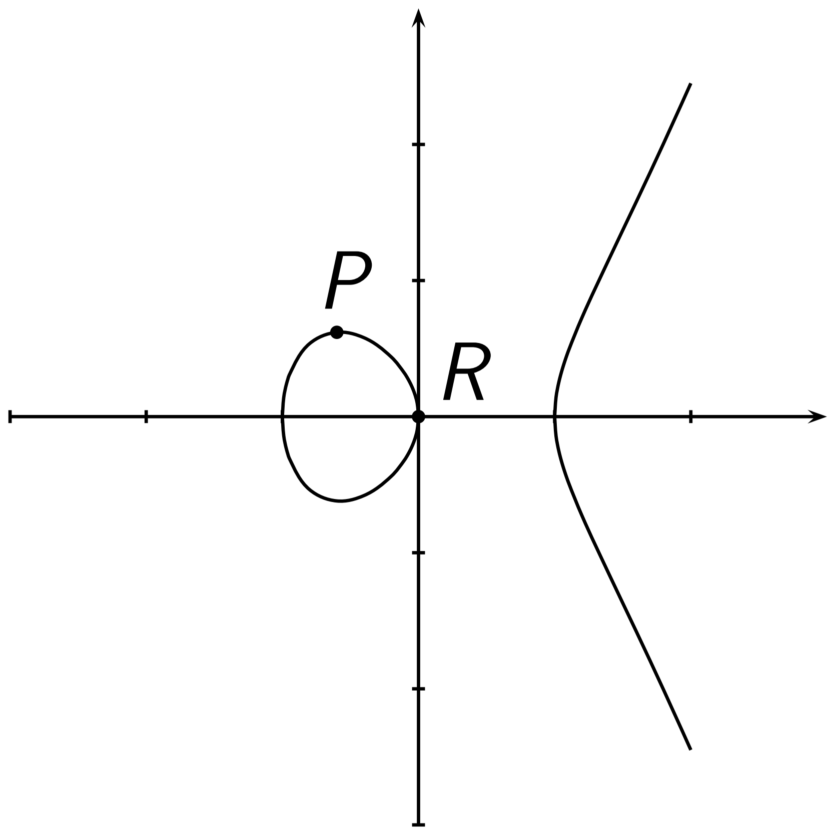
Elliptic curve always has third point on a non-vertical line.

By reduction modulo principal divisors (lines) one can thus reduce any divisor to just $P - \infty$ or the neutral element.

The isomorphism
$\mathrm{Pic}^0_E(\mathbf{F}_{q^k}) \to E(\mathbf{F}_{q^k})$,
$P - \infty \mapsto P, 0 \mapsto \infty$
shows that above construction gives a group on the points of E together with the point at infinity.

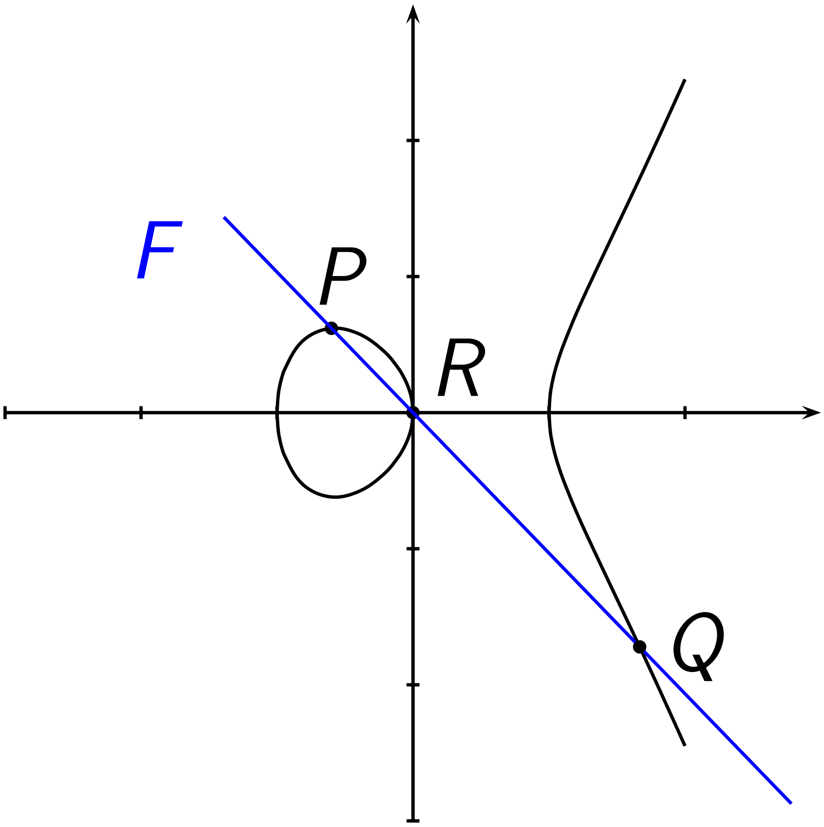
Example: $E(\mathbf{R}), h = 0$

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



Example: $E(\mathbf{R}), h = 0$

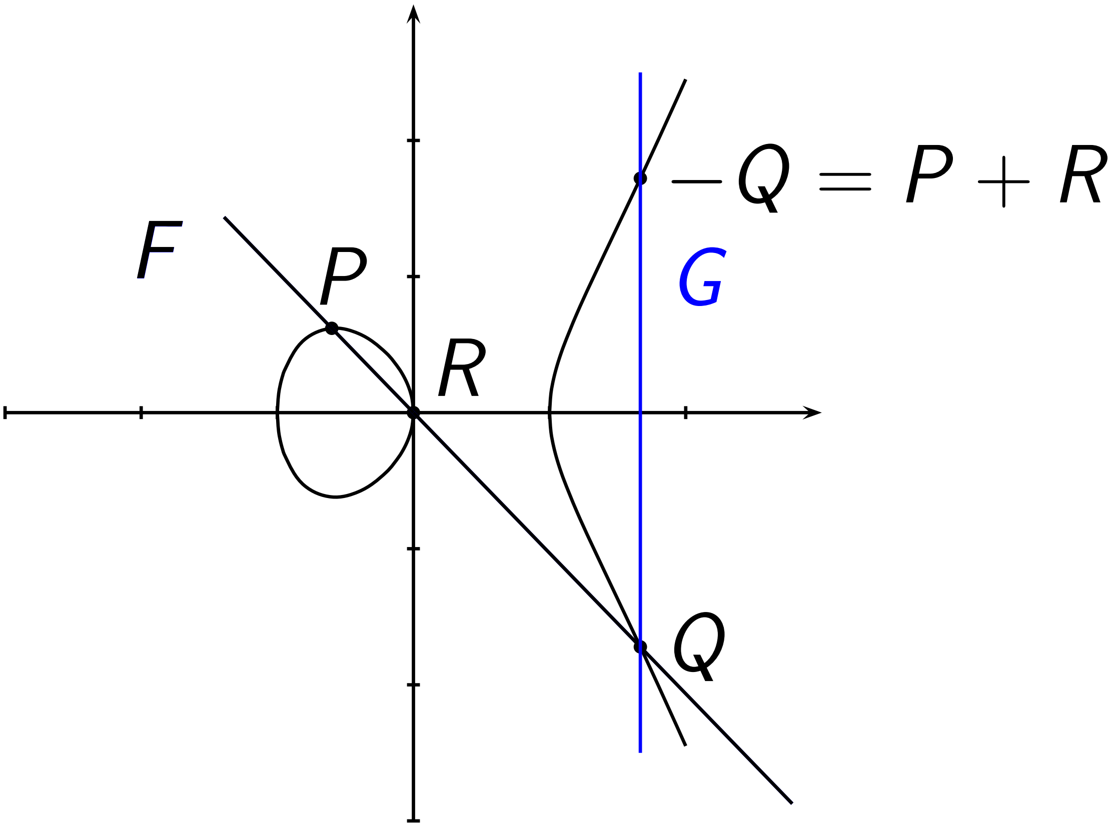
$$y^2 = x^3 - x$$



$$\mathrm{div}(F(x,y)) = P + Q + R - 3\infty$$

Example: $E(\mathbf{R}), h = 0$

$y^2 = x^3 - x$



$$\mathrm{div}(F(x, y)) = P + Q + R - 3\infty$$

$$\mathrm{div}(G(x, y)) = Q + (-Q) - 2\infty$$

Reduced divisors

Divisor D is semi-reduced if

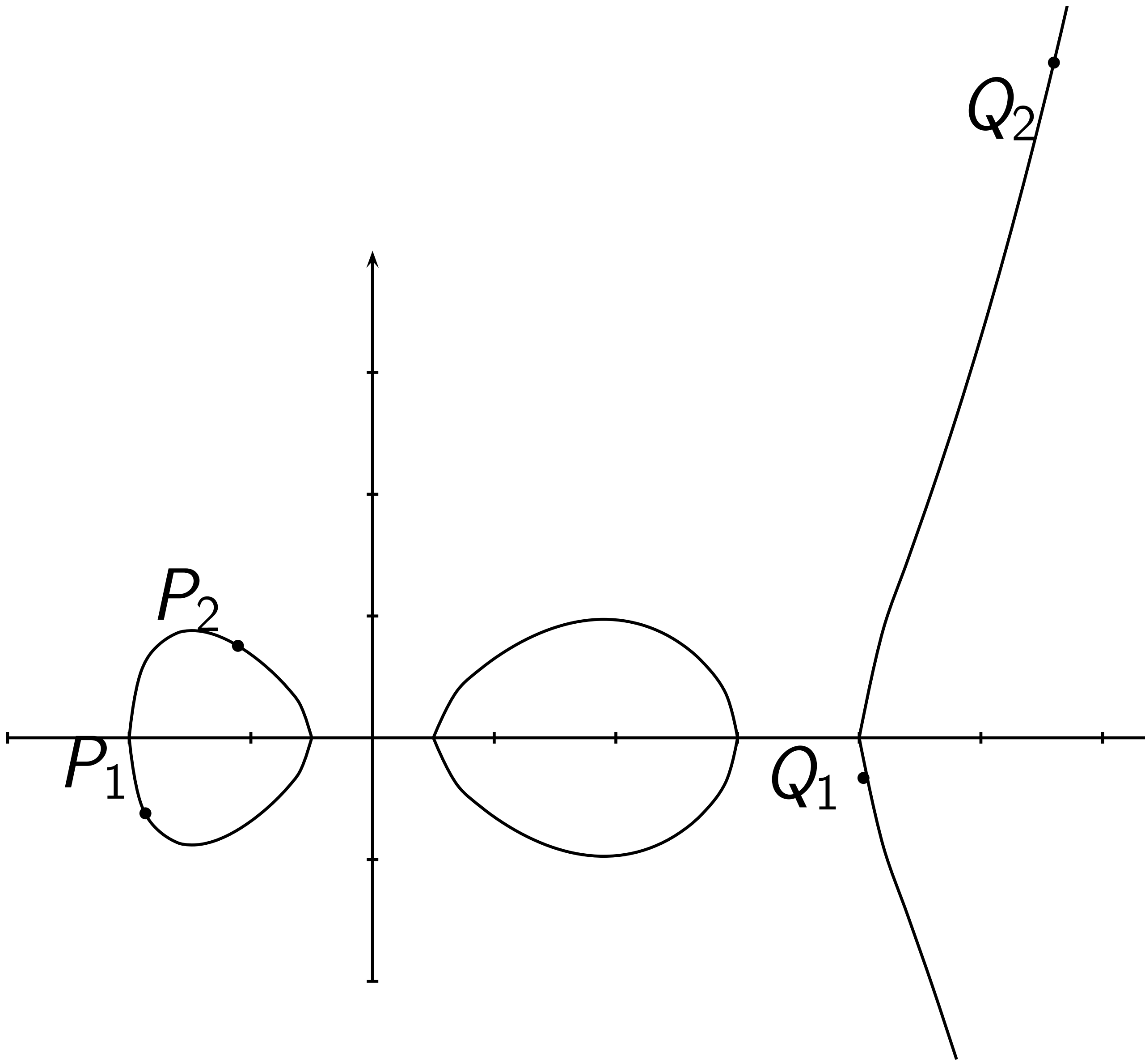
$$D = \sum_{\substack{i=1 \\ P_i \in C(\overline{\mathbf{F}_q}) \setminus \{\infty\}}}^{m} P_i - m\infty$$

and $P_i \neq -P_j$ for $i \neq j$
(no restriction on $\#$ points).

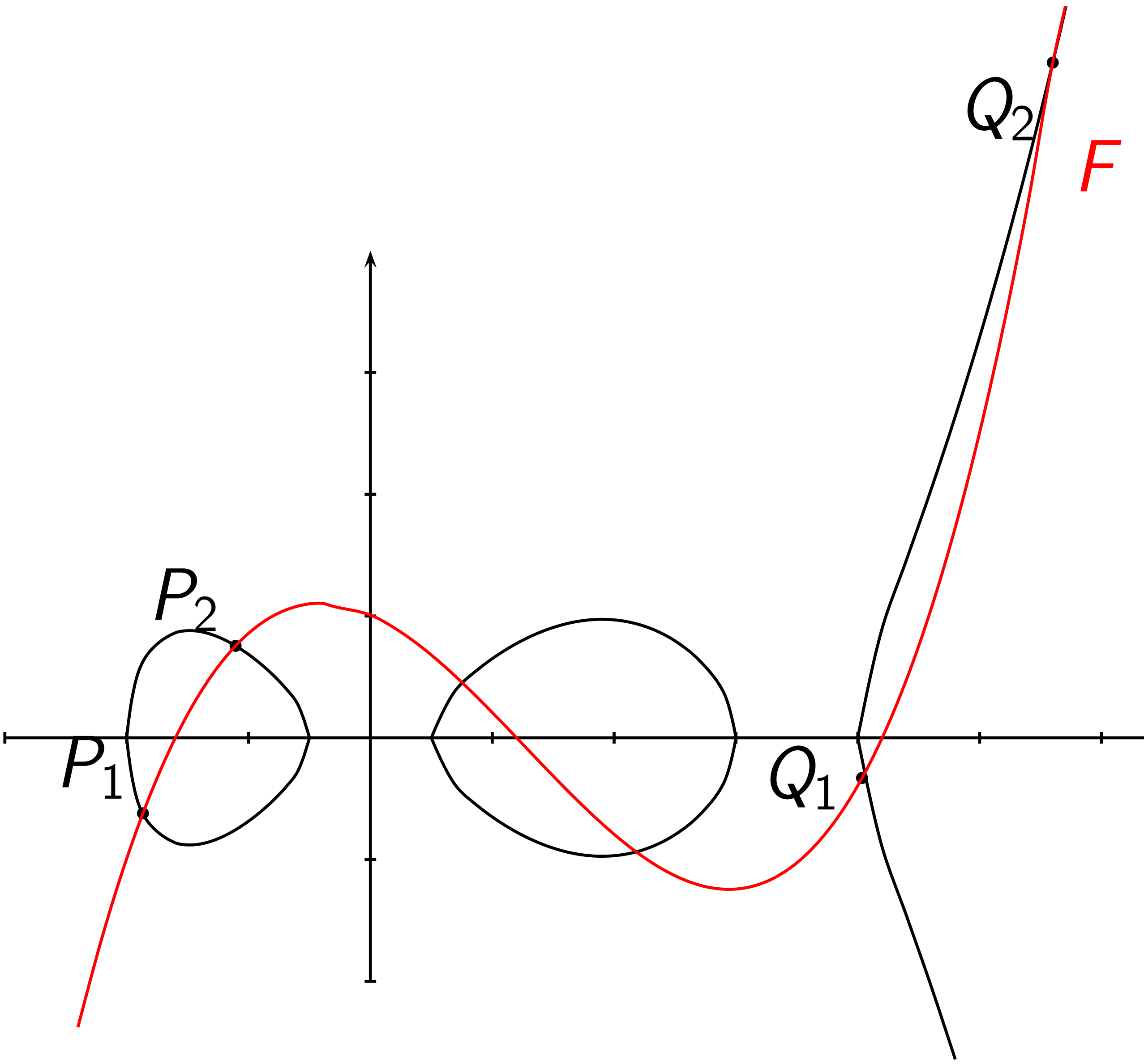
Divisor D is reduced if
it is semi-reduced and $m \leq g$.

Important for representation:
Each divisor class has a unique
reduced representative.

Curve of genus 2 over $\mathbf{R}$, $h = 0$

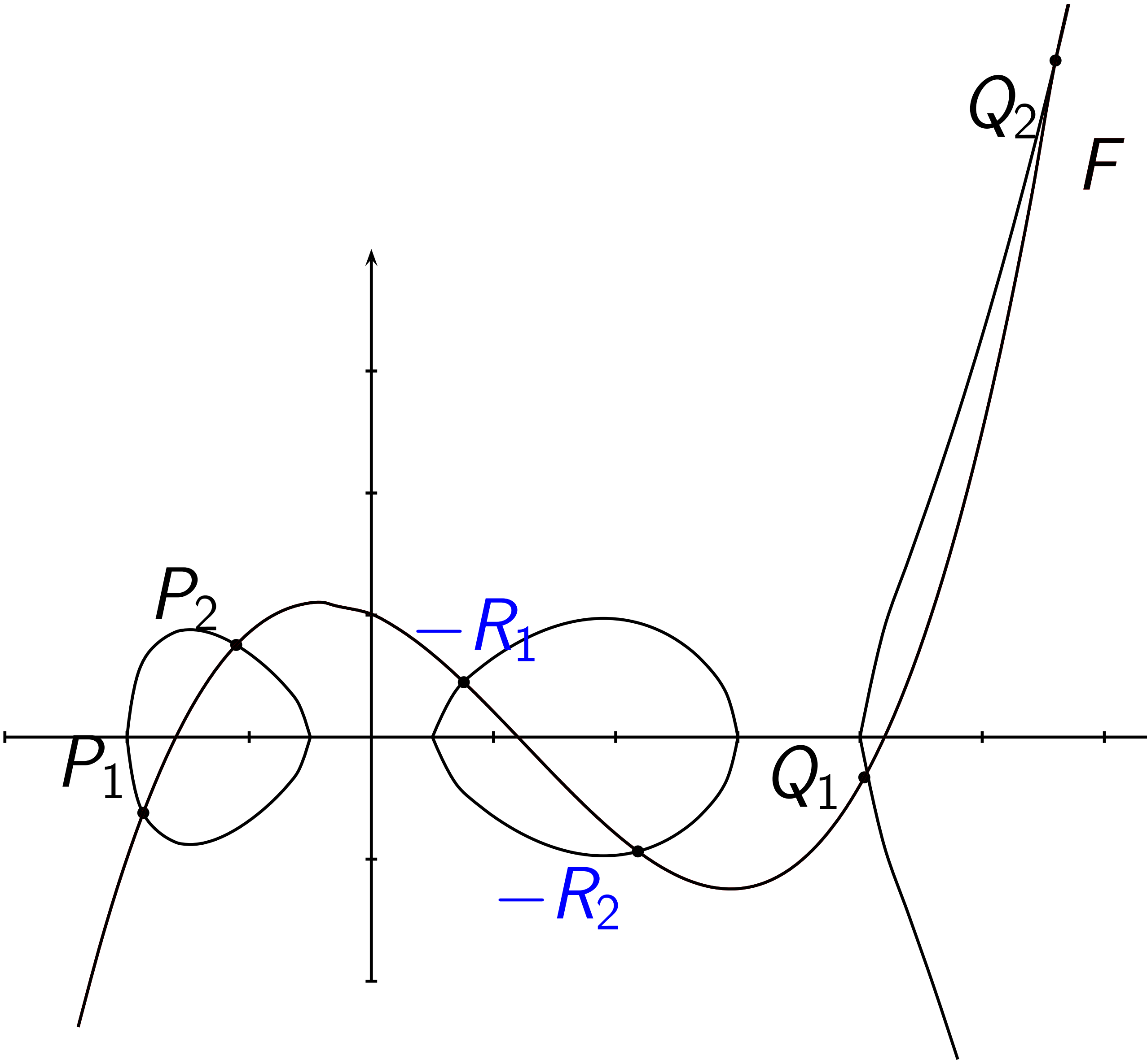


Curve of genus 2 over $\mathbf{R}$, $h = 0$



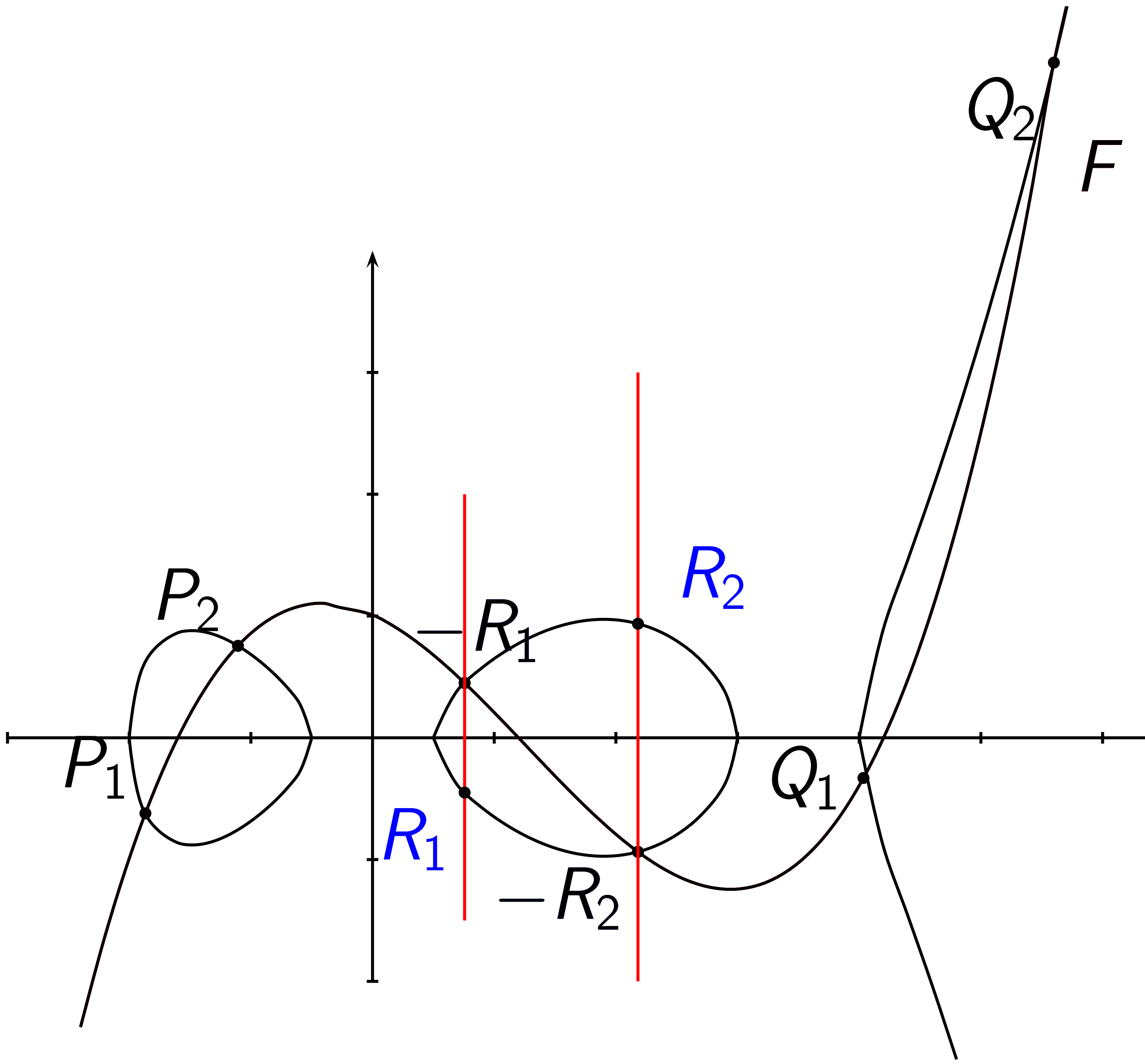
Points on red line (-6∞) form principal divisor

Curve of genus 2 over $\mathbf{R}$, $h = 0$



$$P_1 + P_2 + (-R_1) + (-R_2) + Q_1 + Q_2 - 6\infty = \operatorname{div}(F)$$

Curve of genus 2 over $\mathbf{R}$, $h = 0$



$$\begin{aligned}&(P_1 + P_2 - 2\infty)\\ &\quad + (Q_1 + Q_2 - 2\infty)\\ &= R_1 + R_2 - 2\infty\end{aligned}$$

Still need compact representation.

Idea: use polynomials to represent divisors,
ignore ∞ – multiplicity dictated by affine part.

Let semi-reduced
$D = \sum_{i=1}^{m} P_i - m\infty$
with $P_i = (x_i, y_i)$.

Put $u(x) = \prod_{i=1}^{m}(x - x_i)$
and define v by $v(x_i) = y_i$
with multiplicity (latter gives conditions on derivative of v).

$\deg(v) < \deg(u) = m$.

Reduced divisor: $\deg(u) \leq g$.

Mumford Representation

Easy characterization for field of definition: Class D defined over $\mathbf{F}_q$ has $u, v \in \mathbf{F}_q[x]$.

Divisor classes can be represented by reduced divisors

$\Rightarrow$ each class can be represented by two polynomials

$$[u(x), v(x)]; u, v \in \mathbf{F}_q[x],$$

u monic, $\deg v < \deg u \leq g$,

$$u | v^2 + vh - f.$$

Alternative viewpoint:

Define group on $[u(x), v(x)]$ with conditions as above, according to algorithm on next slide.

Composition (Cantor/Koblitz)

`IN:` $[u_1, v_1], [u_2, v_2]$,

$C : y^2 + h(x)y = f(x)$

`OUT:` $[u, v]$ reduced with

compute $d_1 = \gcd\{u_1, u_2\}$

$= e_1 u_1 + e_2 u_2$;

compute

$d = \gcd\{d_1, v_1 + v_2 + h\}$

$= c_1 d_1 + c_2(v_1 + v_2 + h)$

let $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$

$u = \frac{u_1 u_2}{d^2}$

$v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$

This result $[u, v]$ corresponds to a semireduced divisor.

Reduction (Cantor/Koblitz)

`IN:` $[u_1, v_1], [u_2, v_2]$,

$C : y^2 + h(x)y = f(x)$

`OUT:` $[u, v]$ reduced with

compute $d_1 = \gcd\{u_1, u_2\}$,

$d = c_1 d_1 + c_2(v_1 + v_2 + h)$

let $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$

$u = \frac{u_1 u_2}{d^2}$

$v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$

let $u' = \frac{f - vh - v^2}{u}$

$v' = (-h - v) \bmod u'$

if $\deg u' > g$ put $u = u', v = v'$

repeat u' step

make u monic.

Arithmetic a la Pierrick Gaudry

ePrint Report 2005/314

Fast genus 2 arithmetic based on Theta functions

Needs full 2-torsion group, i.e. cofactor 16.

Shows that approach valid over general fields.

ADD + DBL = 25M,
no inversion!!!
(cf. affine ADD: 22M + 3S + 1I,
DBL: 22M + 5S + 1I)

faster than Montgomery form elliptic curves.

Tate-Lichtenbaum pairing I

$\mathrm{Pic}^0_C(\mathbf{F}_{q^k})[\ell]$:
divisor classes on C of order ℓ
defined over $\mathbf{F}_{q^k}$.

$\bar{D}_1 \in \mathrm{Pic}^0_C(\mathbf{F}_{q^k})[\ell] \Rightarrow \exists F_{D_1}$ such that $\ell D_1 \sim \mathrm{div}(F_{D_1})$, where D_1 represents the class $\bar{D}_1$.

Let $\bar{D}_2 \in \mathrm{Pic}^0_C(\mathbf{F}_{q^k})$ be represented by D_2 with
$\mathrm{support}(D_2) \cap \mathrm{support}(D_1) = \emptyset$.

Tate-Lichtenbaum pairing

$$T_\ell(\bar{D}_1, \bar{D}_2) = F_{D_1}(D_2) = \frac{\prod_{i=1}^n F_{D_1}(P_i)}{\prod_{j=1}^n F_{D_1}(Q_j)}$$

for $D_2 = \sum_{i=1}^n P_i - \sum_{j=1}^n Q_j$.

Tate-Lichtenbaum pairing II

This

$$T_\ell(\bar{D}_1, \bar{D}_2) = F_{D_1}(D_2)$$

defines a bilinear and non-degenerate map T_ℓ :

$$\mathrm{Pic}^0_C(\mathbf{F}_{q^k})[\ell] \times \mathrm{Pic}^0_C(\mathbf{F}_{q^k})/\ell\mathrm{Pic}^0_C(\mathbf{F}_{q^k}) \to \mathbf{F}^*_{q^k}/\mathbf{F}^{*\ell}_{q^k}$$

as ℓ-folds are in the kernel of T_ℓ. Namely, if $\bar{D}_2 = [\ell]\bar{D}_3$ then

$$F_{D_1}(D_2) = F_{D_1}(D_3)^\ell = 1.$$

To achieve unique value in $\mathbf{F}_{q^k}$ rather than class do final exponentiation

$$\tilde{T}_\ell = T_\ell(\bar{D}_1, \bar{D}_2)^{(q^k-1)/\ell}.$$

Tate-Lichtenbaum pairing III

For elliptic curves use isomorphism

$$\mathrm{Pic}^0_E(\mathbf{F}_{q^k}) \cong E(\mathbf{F}_{q^k})$$

to define pairing on points $T_\ell(P, Q)$, with $D_1 = P - \infty$, $D_2 = (Q + R) - R$ for some R.

Build F iteratively by Miller's algorithm (double-and-add).

Often

$$T_\ell : E(\mathbf{F}_{q})[\ell] \times E(\mathbf{F}_{q^k})/\ell E(\mathbf{F}_{q^k}) \to \mathbf{F}^*_{q^k}$$

Miller's algorithm

$\texttt{IN}$: $\ell = \sum_{i=0}^{n-1} \ell_i 2^i$, $P, Q+R, R$

$\texttt{OUT}$: $T_\ell(P,Q)$

$T \leftarrow P$, $F \leftarrow 1$

for $i = n-2$ downto 0 do

  Calculate l and v in doubling

  $T \leftarrow 2T$

$F \leftarrow F^2 \cdot l(Q+R)v(R)/(l(R)v(Q+R))$

  if $\ell_i = 1$ then

  Calculate l and v in addition

$T + P$

  $T \leftarrow T + P$

$F \leftarrow F \cdot l(Q+R)v(R)/(l(R)v(Q+R))$

return F

Weil pairing

For elliptic curve E define
$W_\ell : E(\overline{\mathbf{F}}_q)[\ell] \times E(\overline{\mathbf{F}}_q)[\ell] \to \mu_\ell$,
$(P, Q) \mapsto (F_{P-\infty}(D_Q))/(F_{Q-\infty}(D_P))$,
where μ_ℓ is the multiplicative groups of the ℓ-th roots of unity in the algebraic closure $\overline{\mathbf{F}}_q$ of $\mathbf{F}_q$.
Obviously, $W_\ell(P, P) = 1$.

Weil pairings $\sim$ two-fold application of Tate-Lichtenbaum pairing, note $Q \in E(\mathbf{F}_{q^k})$.

If $k = 1$ then the Weil pairing is trivial & one needs to use larger field.

Edwards are great for . . .

. . . fast implementations
of scalar multiplication nP.

. . . lazy implementations
of scalar multiplication nP.

. . . secure implementations
of scalar multiplication nP.

. . . teaching elliptic curves.

. . . everything

Edwards are great for . . .

. . . fast implementations
of scalar multiplication nP.

. . . lazy implementations
of scalar multiplication nP.

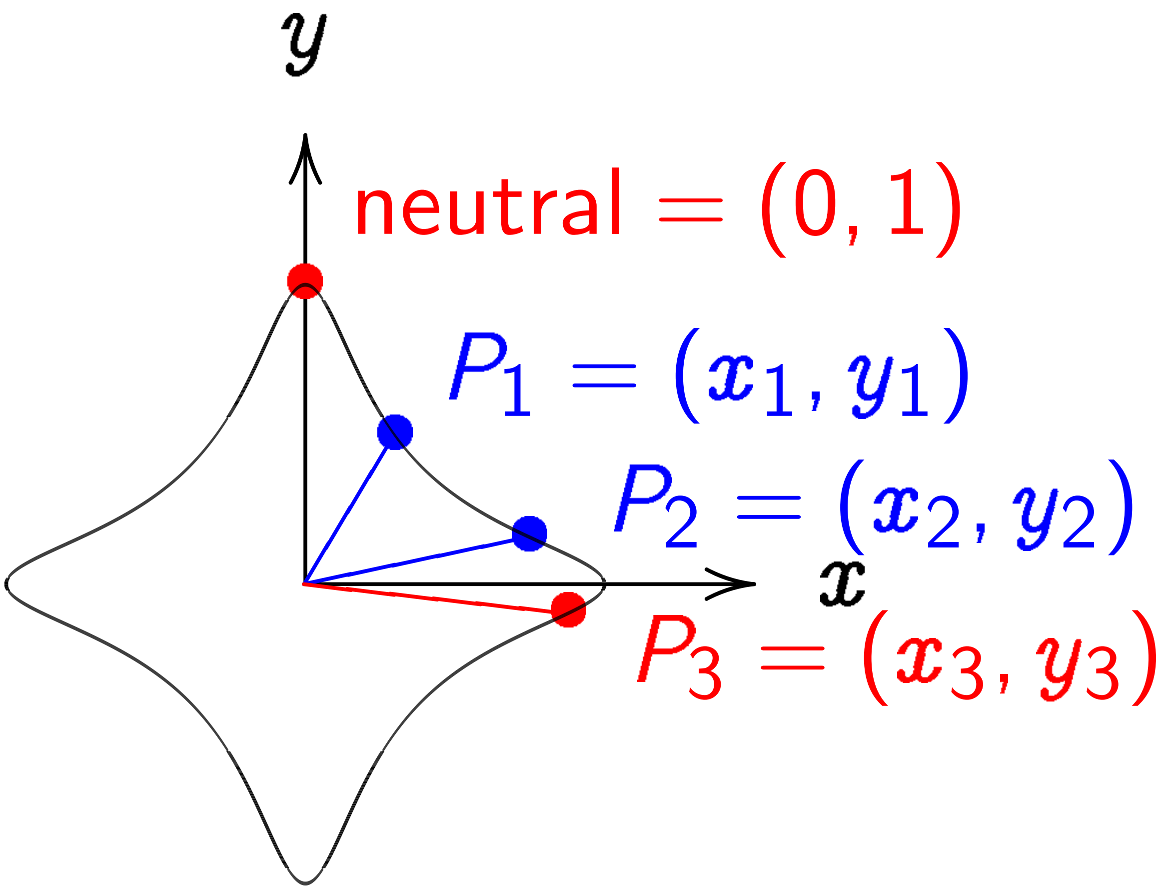
. . . secure implementations
of scalar multiplication nP.

. . . teaching elliptic curves.

. . . everything?

How about pairings? Loop shortening etc. does not depend on curve representation; but how to compute the Miller function? How to compute the analogue of the line functions?

Geometric addition law



Would like to find function $g_{R,P}$ depending on input points P, R with

$$\operatorname{div}(g_{R,P}) = \operatorname{div}(f_1/f_2) = R + P - (0,1) - (R + P)$$

Equation has degree 4
$E : x^2 + y^2 = 1 + dx^2y^2$.

Bezout:
$4\deg(f)$ intersection points
of E and graph of f.

$\deg(f_i) = 1$: gives 4 points;
need to eliminate 2 out of each.

$\deg(f_i) = 2$: gives 8 points;
could offer enough freedom of
cancellation.

Problem: conic is determined by
5 points; not enough control over
intersection points.

Interlude

Projective Edwards curves
$Z^2(X^2+Y^2) = Z^4 + dX^2Y^2$
have points $(X : Y : Z)$.
Affine (x, y) maps to $(X : Y : 1)$.

Other points must have $Z = 0$:
$0^2(X^2+Y^2) = 0^4 + dX^2Y^2$,
thus $0 = dX^2Y^2$.

This gives 2 points:
$\Omega_1 = (0 : 1 : 0)$, $\Omega_2 = (1 : 0 : 0)$.

No trouble with arithmetic:
these are singular & blow up
to two points over $k(\sqrt{d})$.

Conic sections

Solution: Ω_1 and Ω_2 are singular and have multiplicity 2.

Determine conic via 5 points:

$P_1, P_2, (0,-1), \Omega_1$, and Ω_2.

This has shape

$f_1 = c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ$,

where $(c_{Z^2} : c_{XY} : c_{XZ}) \in \mathbf{P}^2(K)$

depend on P_1 and P_2.

These count for

7 intersection points,

only one more point R.

Divisor of f_1 is
$P_1 + P_2 + (0, -1) + \Omega_1 + \Omega_2 + R$.

Use f_2 to "replace"
$(0, -1)$ by $(0, 1)$ and
$-R$ by $P_1 + P_2 = (X_3 : Y_3 : Z_3)$.

Put $f_2 = l_1 \cdot l_2$, with
$l_1 = Z_3 Y - Y_3 Z$ and $l_2 = X$.

These also eliminate
Ω_1 and Ω_2, thus
$\operatorname{div}(f_1/f_2) = P_1 + P_2 - P_3 - (0, 1)$

Theorem

If $P_1 \neq P_2$, $P_1 \neq (0,1)'$ and $P_2 \neq (0,1)'$, then

$$c_{Z^2} = X_1X_2(Y_1Z_2 - Y_2Z_1),$$

$$c_{XY} = Z_1Z_2(X_1Z_2 - X_2Z_1 + X_1Y_2 - X_2Y_1),$$

$$c_{XZ} = X_2Y_2Z_1^2 - X_1Y_1Z_2^2 + Y_1Y_2(X_2Z_1 - X_1Z_2).$$

If $P_1 \neq P_2 = (0,1)'$, then

$c_{Z^2} = -X_1$, $c_{XY} = Z_1$, $c_{XZ} = Z_1$.

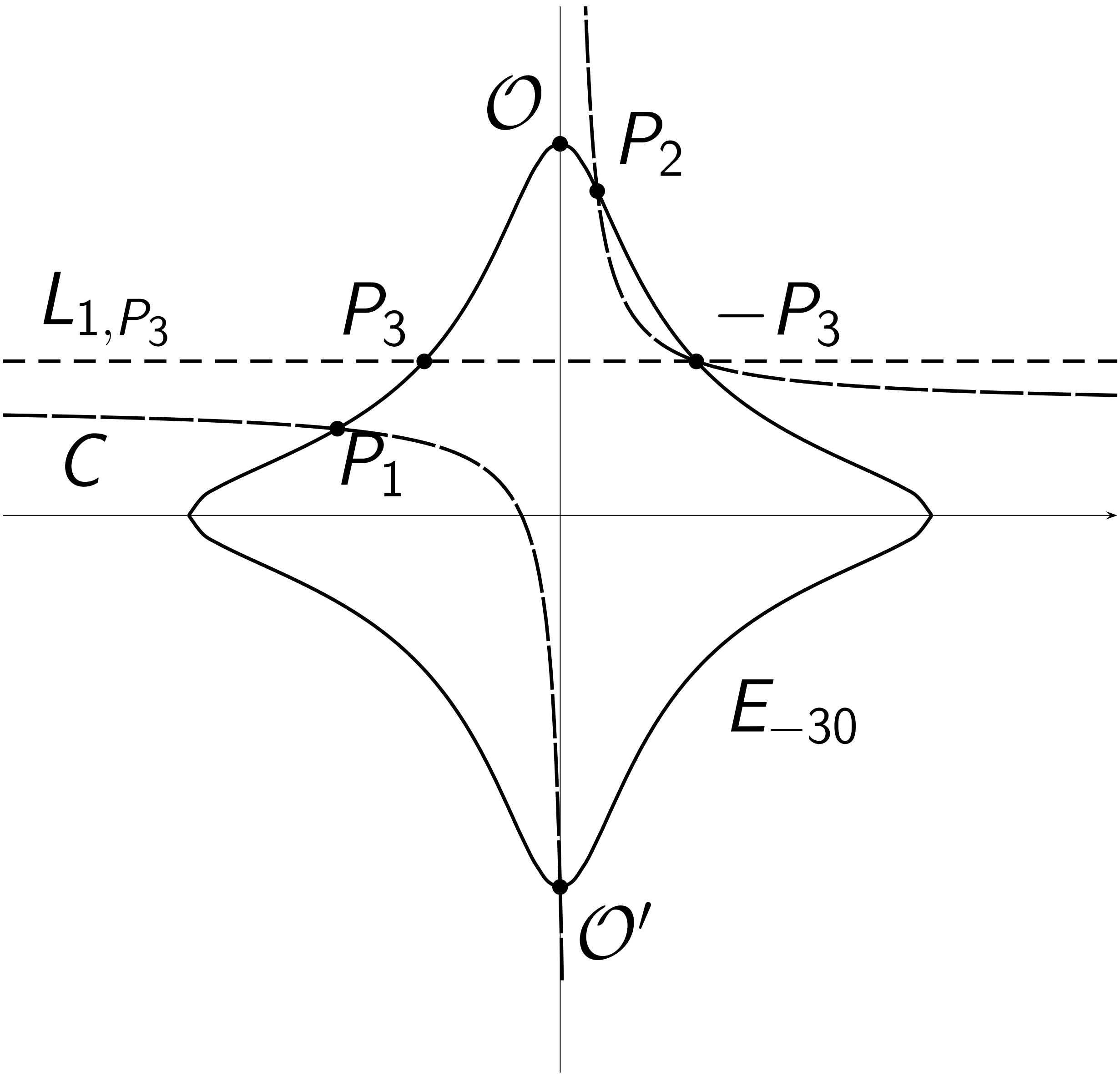
If $P_1 = P_2$, then

$$c_{Z^2} = X_1Z_1(Z_1 - Y_1),$$

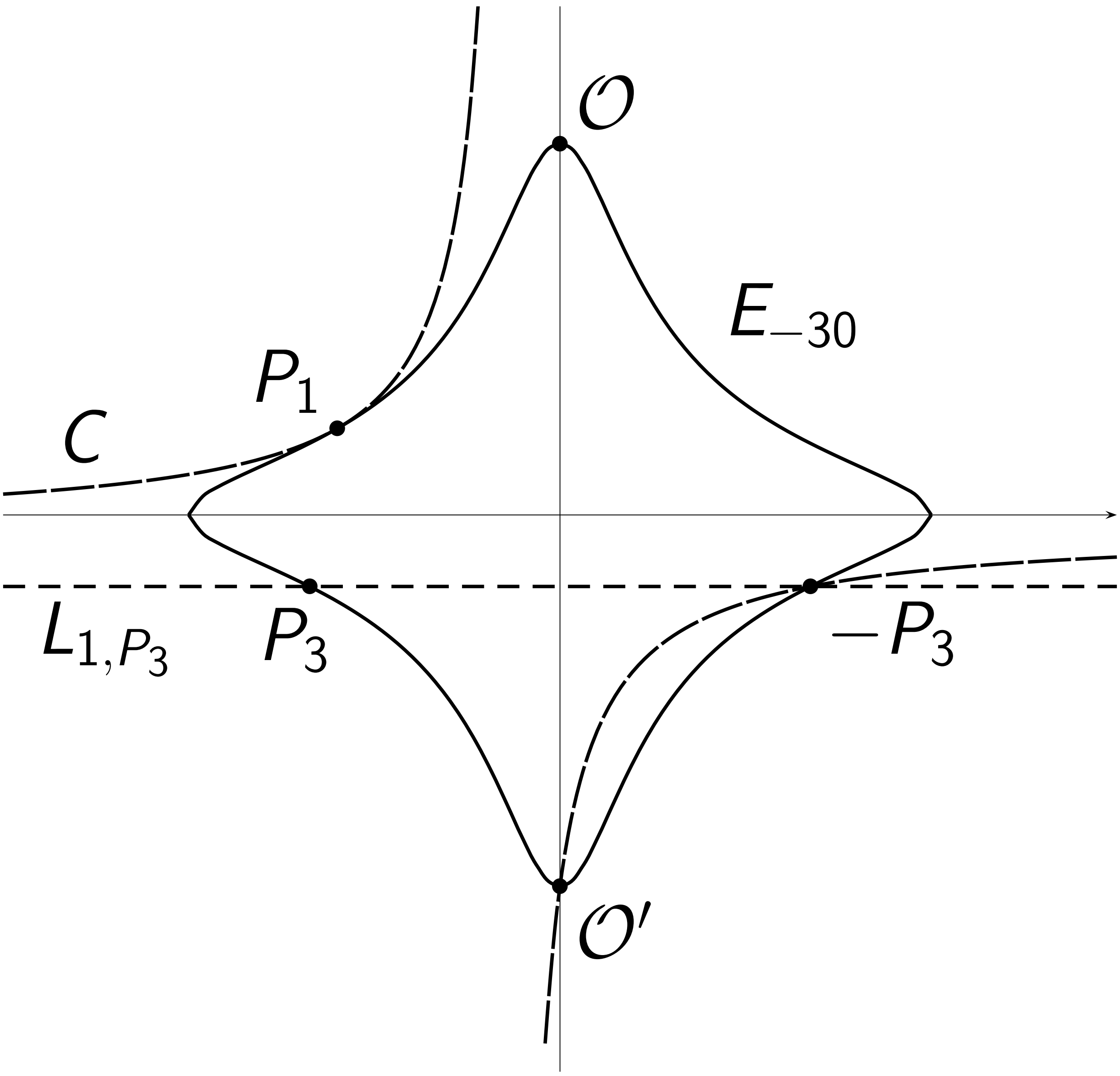
$$c_{XY} = dX_1^2Y_1 - Z_1^3,$$

$$c_{XZ} = Z_1(Z_1Y_1 - aX_1^2).$$

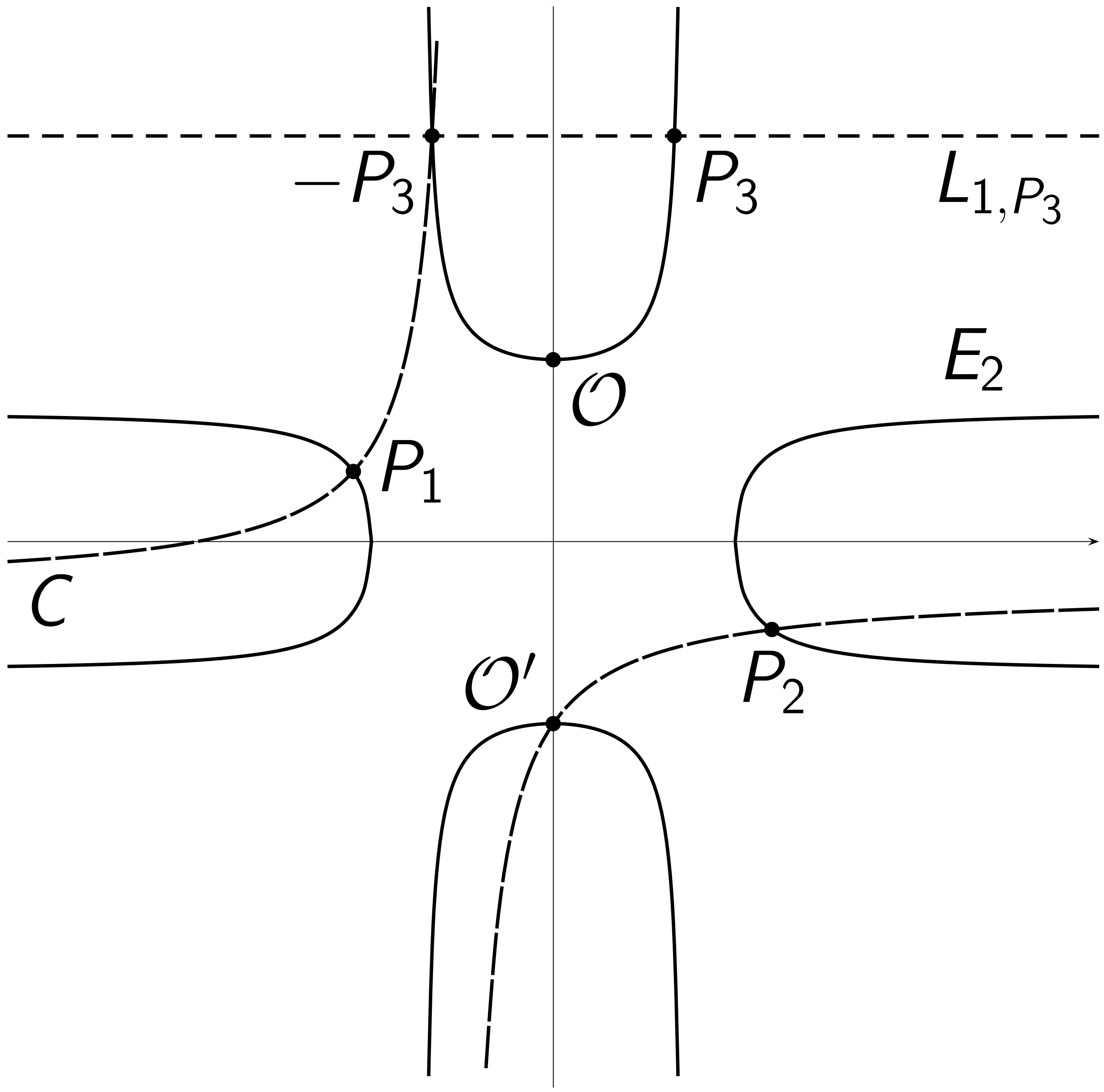
Addition over $\mathbf{R}$, $d < 0$



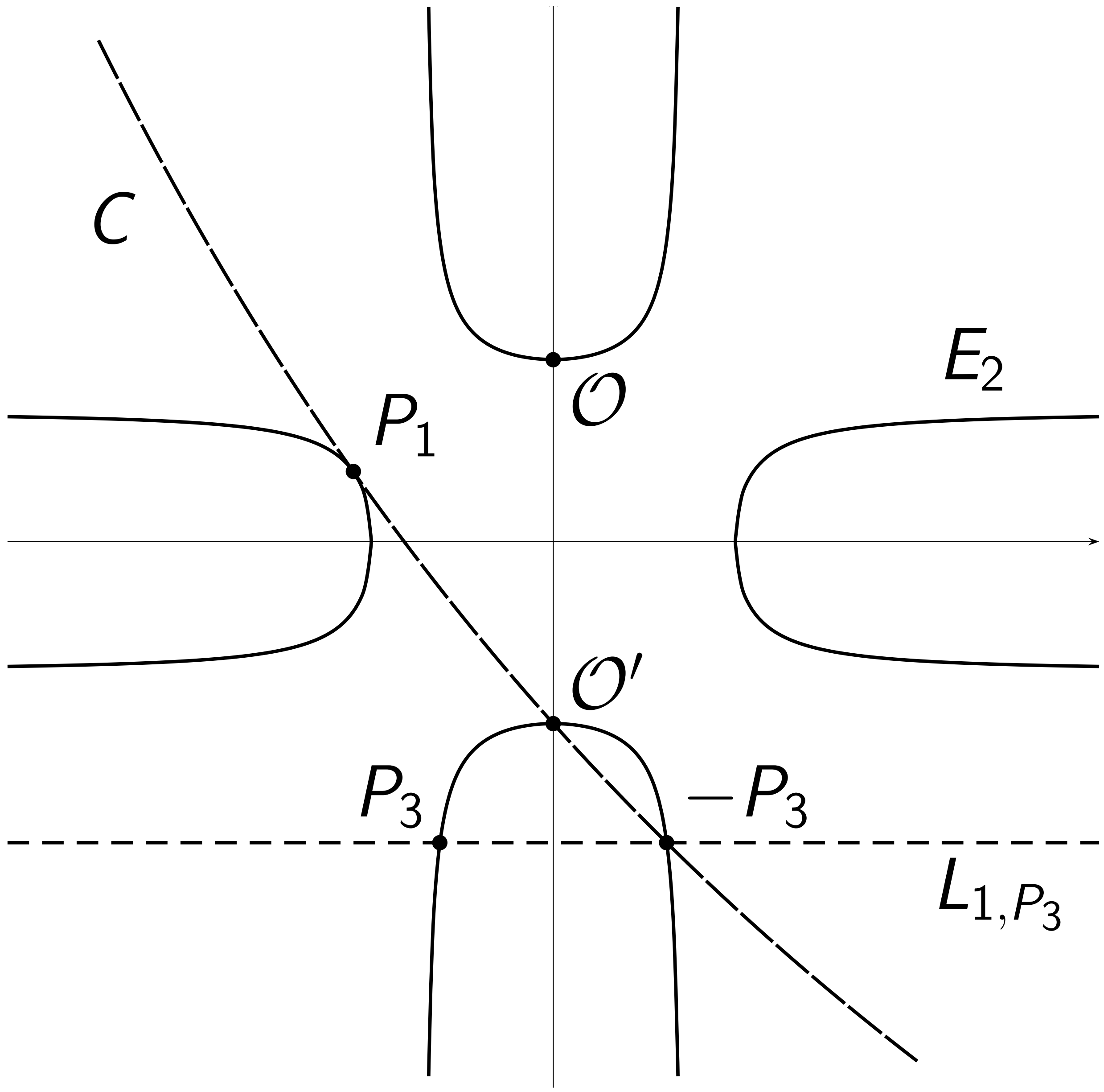
Doubling over **R**, $d < 0$



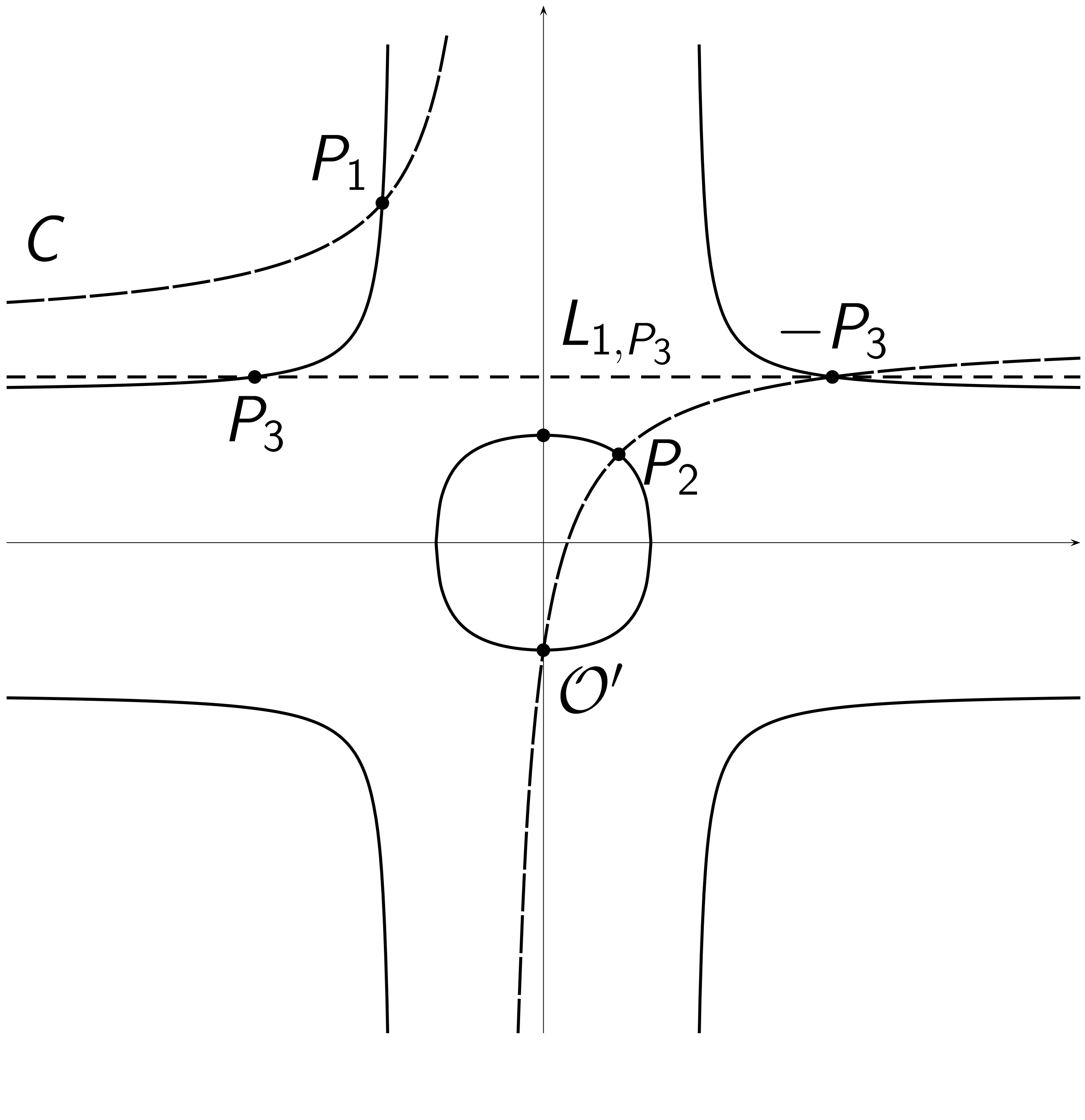
Addition over **R**, $d > 1$



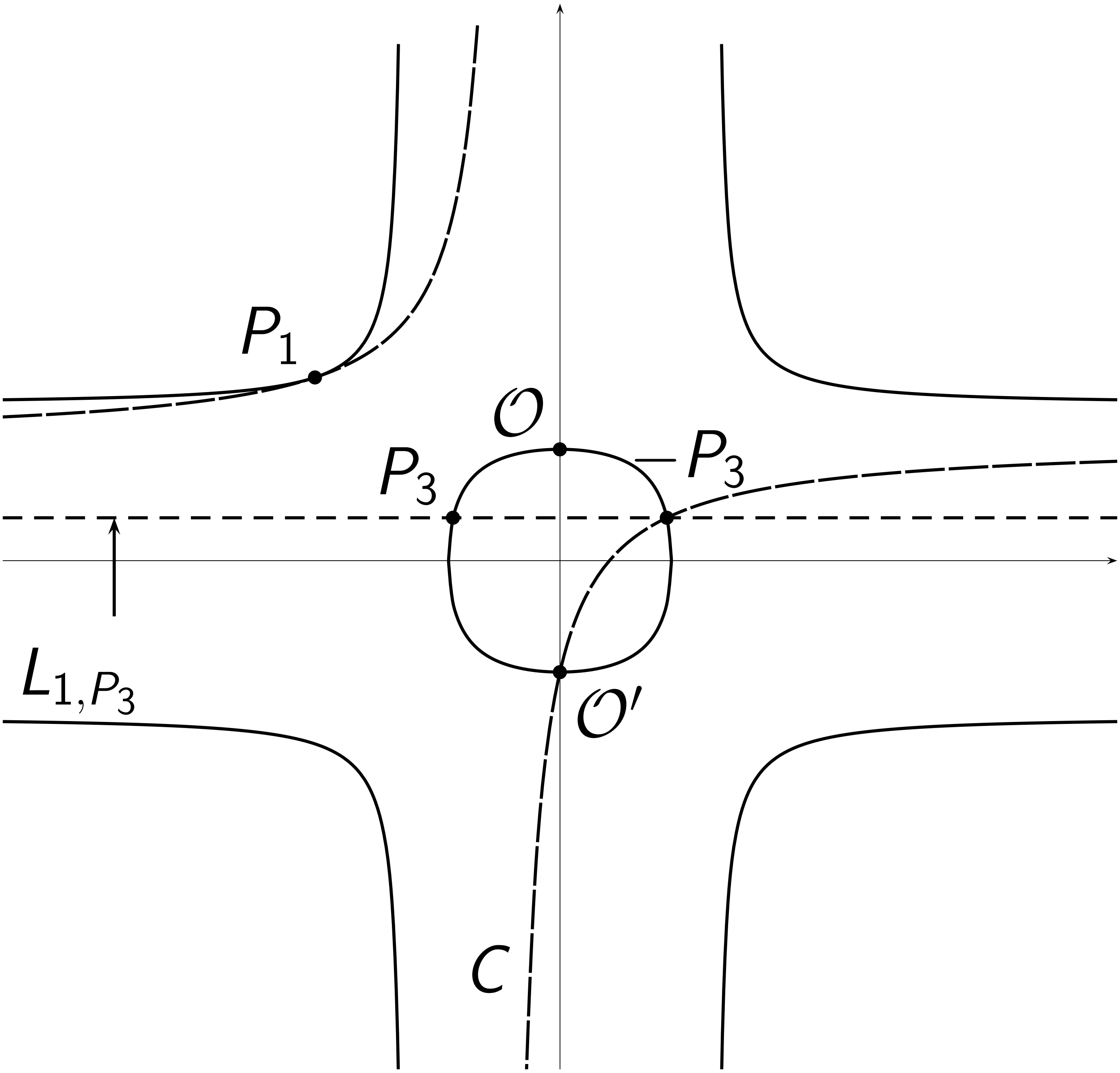
Doubling over **R**, $d > 1$



Addition over $\mathbf{R}$, $0 < d < 1$



Doubling over **R**, $0 < d < 1$



Summary of other attacks

Definition of embedding degree does not cover all attacks.
For $\mathbf{F}_{p^n}$ watch out that pairing can map to $\mathbf{F}_{p^{km}}$ with $m < n$.
Watch out for this when selecting curves over $\mathbf{F}_{p^n}$!

Anomalous curves:
If $E/\mathbf{F}_p$ has $\#E(\mathbf{F}_p) = p$ then transfer $E(\mathbf{F}_p)$ to $(\mathbf{F}_p, +)$.
Very easy DLP.
Not a problem for Koblitz curves, attack applies to order-p subgroup.

Weil descent:
Maps DLP in E over $\mathbf{F}_{p^{mn}}$
to DLP on variety J over $\mathbf{F}_{p^n}$.
J has larger dimension; elements represented as polynomials of low degree. $\Rightarrow$ index calculus.

This is efficient if dimension of J is not too big.

Particularly nice to compute with J if it is the Jacobian of a hyperelliptic curve C.
For genus g get complexity $\tilde{O}(p^{2-\frac{2}{g+1}})$ with the factor base described before, since polynomials have degree $\leq g$.