# Pairing Based Cryptography

Tanja Lange

Department of Mathematics

Technical University of Denmark

t.lange@mat.dtu.dk

04.12.2005

# Overview

- Protocols
- Elliptic curves
  - Definition and group law
  - Divisor class group (explanation of group law, example hyperelliptic curves)
- Weil and Tate pairing on elliptic curves
- Efficient computation of pairings
- Supersingular and ordinary elliptic curves
- Distortion maps
- Embedding degree
- MNT curves
- Outlook

# Protocols

# Diffie-Hellman Key exchange

**Alice**

1. secretly generates $a < |\langle P \rangle|$
2. computes $Q_1 = [a]P$
3. transmits $Q_1$
4. computes $[a]Q_2$

**Bob**

1. secretly generates $b < |\langle P \rangle|$
2. computes $Q_2 = [b]P$
3. transmits $Q_2$
4. computes $[b] \cdot Q_1$

$$[a]Q_2 = [ab]P = [b] \cdot Q_1$$

**Common Key:** the group element $k = [(ab)]P \in G$ can be used in symmetric encryption.

# ElGamal Encryption

Public parameters:
Group $G$, generator $P$, $\mathrm{ord}(P) = l$, some invertible embedding function $H : m \to G$.
Receiver has secret key $s_A$ and public key $P_A = [s_A]P$.

- Encrypt message $m$
  - choose random integer $k$
  - compute $R = [k]P$ and $c = H(m) + [k]P_A$
- Decrypt ciphertext $(R, c)$
  - compute $S = [s_A]R$
  - obtain $m = H^{-1}(c - S)$

  (This gives $m$ as $S = [s_A]R = [ks_A]P = [k]P_A$).

# DL systems

These systems assume that the Discrete Logarithm Problem (DLP) is hard to solve, i.e.

- given $P$ and $P_A = [s_A]P$
- it is hard to find $s_A$.

The Computational Diffie-Hellman Problem (CDHP) is the problem

- given $P$, $P_A = [s_A]P$, and $P_B = [s_B]P$
- compute $[s_A s_B]P$.

The Decisional Diffie-Hellman Problem (DDHP) is the problem

- given $P$, $P_A = [s_A]P$, $P_B = [s_B]P$ and $R = [r]P$
- decide whether $R = [s_A s_B]P$.

# Pairings

Let $(G_1, +), (G_1', +)$ and $(G, \cdot)$ be groups and let

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

be a map satisfying

- $e(P + Q, R') = e(P, R')e(Q, R')$
- $e(P, R' + S') = e(P, R')e(P, S')$
- The map is non-degenerate in the first argument, i.e. if $e(P, R') = 1$ for all $R' \in G_1'$ for some $P$ then $P$ is the identity in $G_1$

Then $e$ is called a bilinear map or pairing.

In protocol papers often $G_1 = G_1'$.

# Consequences

- Assume that $G_1 = G_1'$ and hence

$$e(P, P) \neq 1.$$

Then for all triples $(P_1, P_2, P_3) \in \langle P \rangle^3$ one can decide in time polynomial in $\log \ell$ whether

$$\log_P(P_3) = \log_P(P_1) \log_P(P_2)$$

by comparing

$$e(P_1, P_2) \stackrel{?}{=} e(P, P_3).$$

Thus the DDHP is easy.

- The DL system $G_1$ is at most as secure as the system $G$. Even if $G_1 \neq G_1'$ one can transfer the DLP in $G_1$ to a DLP in $G$, provided that one can find an element $P' \in G_1'$ such that the map $P \to e(P, P')$ is injective.

# 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 $[a]P, [a]P'$.
- Upon receipt of $[b]P$ and $[c]P'$ put $k = (e([b]P, [c]P'))^a$

The resulting element $k$ is the same for each participant as

$$k = (e([b]P, [c]P'))^a = (e(P, P'))^{abc} = (e([a]P, [c]P'))^b = (e([a]P, [b]P'))^c.$$

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

# Pairing based protocols II

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

Idea: sender decides public key of receiver (i.e. using his email-address).

Consequences

- Advantage if recipient is not in system or sender wants to force use of a fresh key (other applications possible).
- Set-up requires a trusted authority (TA) which can compute the secret key for a given public key.

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

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

# ID-based cryptography II

Encryption:

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

Decryption

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

$$e(R, S') = e([k]P, [s]H(ID)) = (e(P, H(ID)))^{ks} = (e([s]P, H(ID)))^k$$

$$\Rightarrow c \oplus e(R, S') = c \oplus (e(P_{pub}, H(ID)))^k = m$$

# Security assumptions

- Clearly these systems require that the DLP is hard in the groups.
- Additionally we define the following computational and decisional problem:
  - Computational Bilinear Diffie-Hellman Problem (CBDHP):
    Compute $[s_A s_B s_C]P$ given $[s_A]P, [s_B]P, [s_C]P$ and $P$
  - Decisional Bilinear Diffie-Hellman Problem (DBDHP):
    Given $P, [s_A]P, [s_B]P, [s_C]P$ and $[r]P$ decide whether $[r]P = [s_A s_B s_C]P$.

# Arithmetic on elliptic curves

# Elliptic curve

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)}y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)},\ \ h, f \in \mathbb{F}_q[x].$$

**Group:** $E(\mathbb{F}_q) = \{\, (x, y) \in \mathbb{F}_q^2 \,:\, y^2 + h(x)y = f(x) \,\} \cup \{\, P_\infty \,\}$

Often $q = 2^r$ or $q = p$, prime. Isomorphic transformations lead to

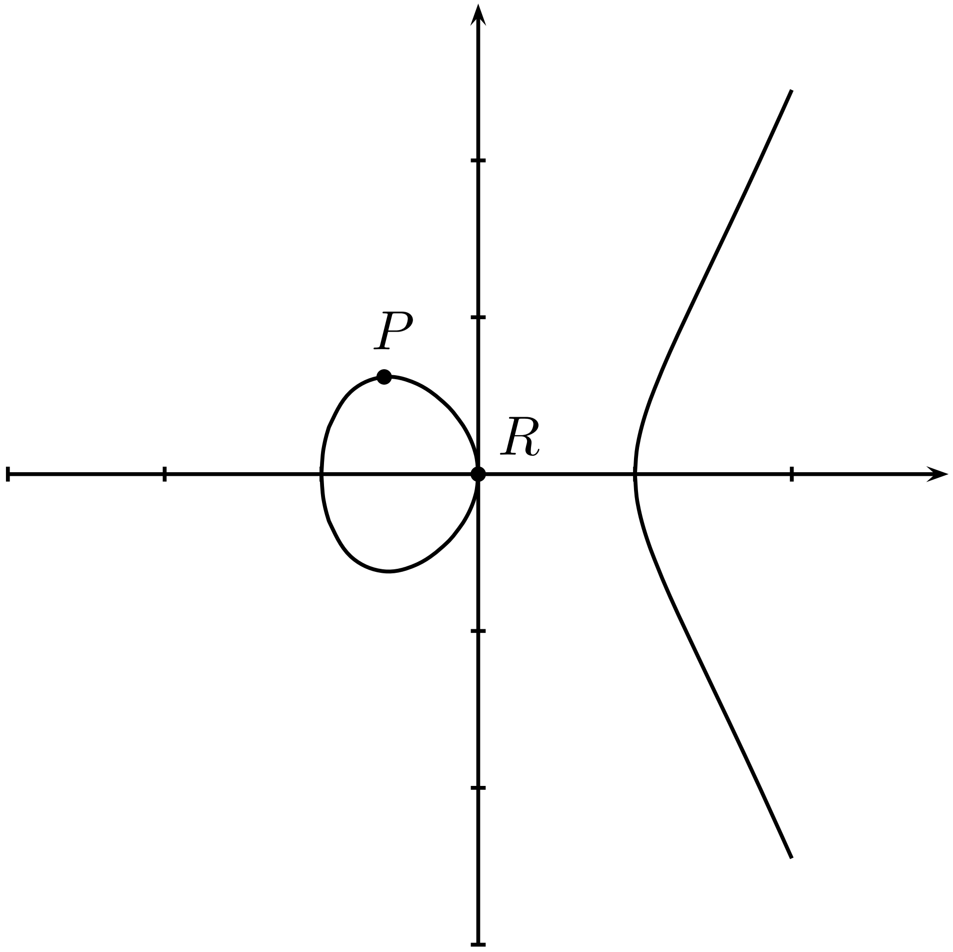
$y^2 = f(x)$ $\quad$ $q$ odd,

for

$$\begin{aligned} y^2 + xy &= x^3 + a_2x^2 + a_6 \\ y^2 + y &= x^3 + a_4x + a_6 \end{aligned} \qquad q = 2^r,\quad \begin{array}{l}\text{curve non-supersingular} \\ \text{curve supersingular}\end{array}$$

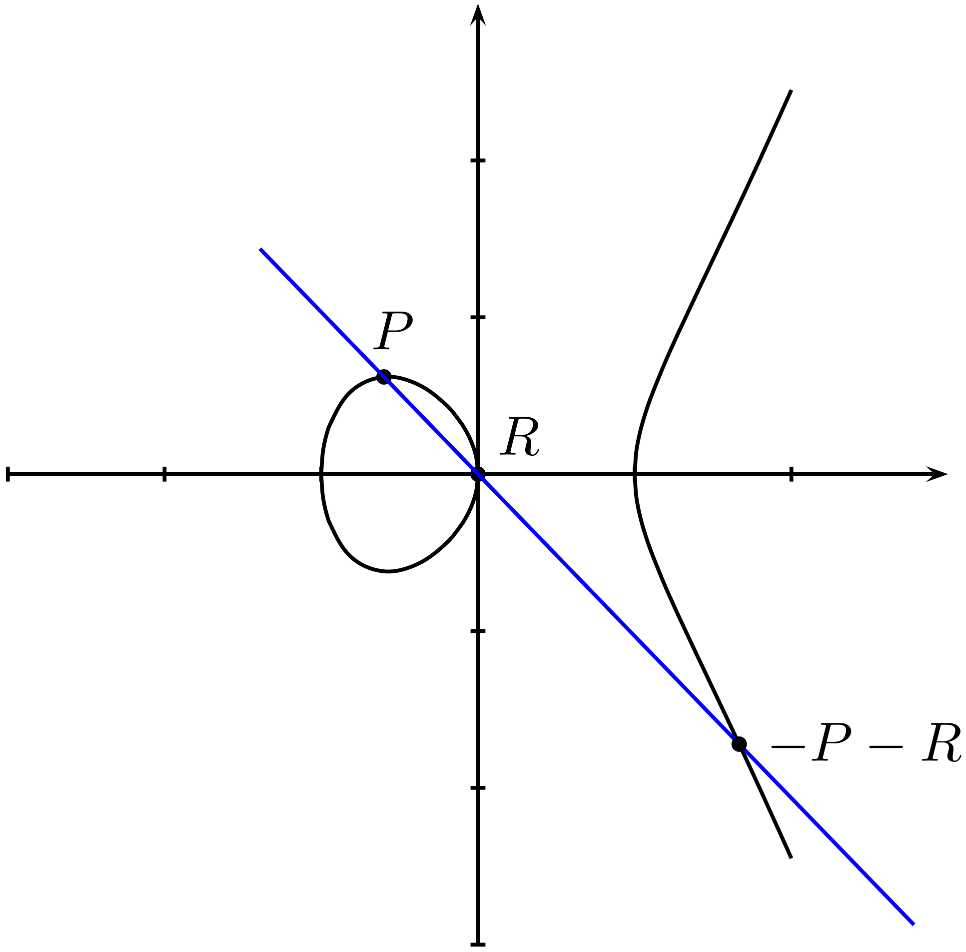
# Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$

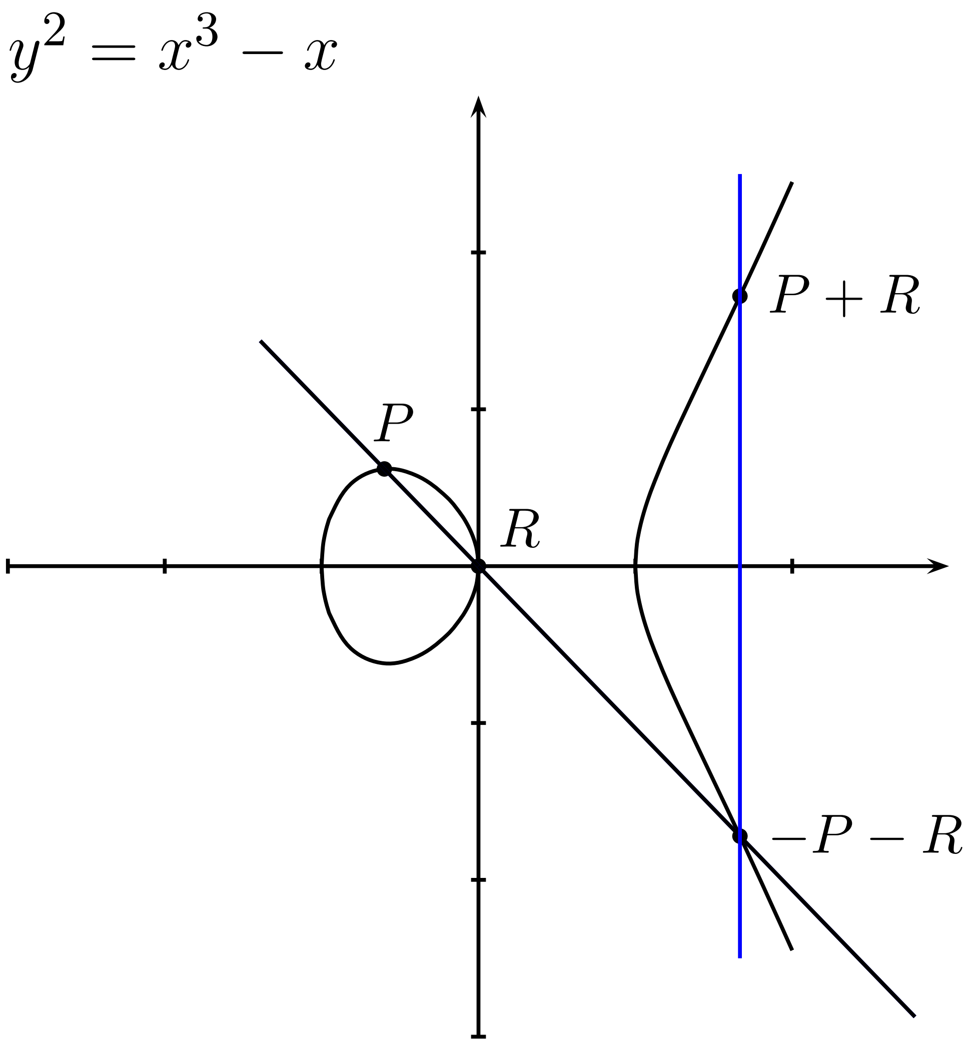


# Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$

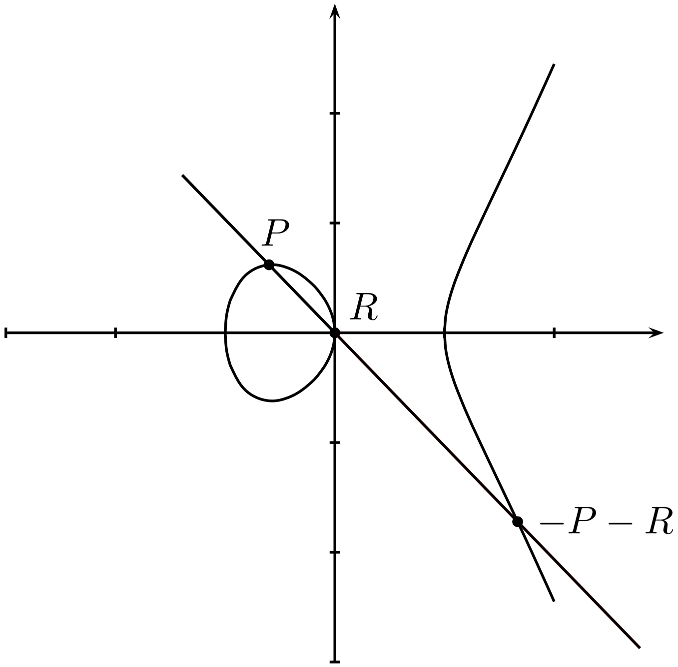


# Group Law in $E(\mathbb{R}), h = 0$



# Group Law ($q$ odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$




Line $y = \lambda x + \mu$ has slope

$$\lambda = \frac{y_R - y_P}{x_R - x_P}.$$

Equating gives

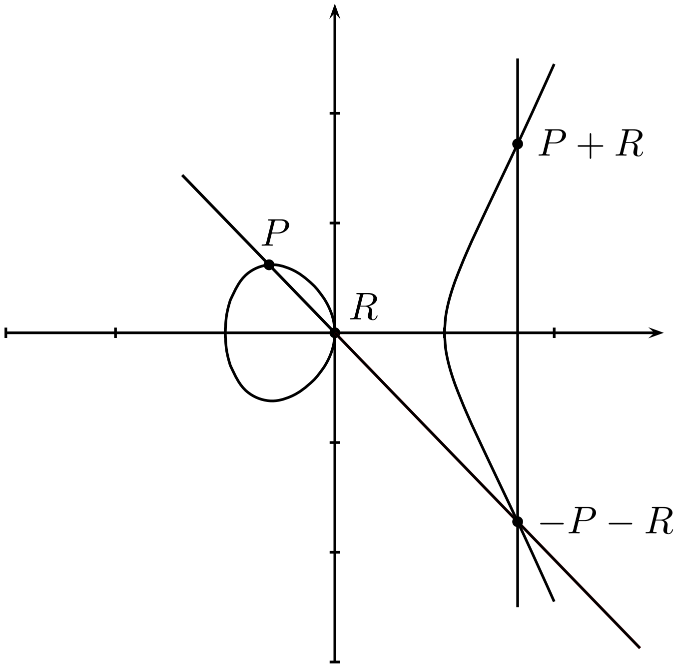
$$(\lambda x + \mu)^2 = x^3 + a_4 x + a_6.$$

This equation has 3 solutions, the $x$-coordinates of $P$, $R$ and $-P-R$, thus

$$\begin{aligned}(x - x_P)(x - x_R)(x - x_{-P-R}) &= x^3 - \lambda^2 x^2 + (a_4 - 2\lambda\mu)x + a_6 - \mu^2 \\ x_{-P-R} &= \lambda^2 - x_P - x_R\end{aligned}$$

# Group Law ($q$ odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$




Point $P$ is on line, thus

$$y_P = \lambda x_P + \mu, \text{ i.e.}$$
$$\mu = y_P - \lambda x_P,$$

and

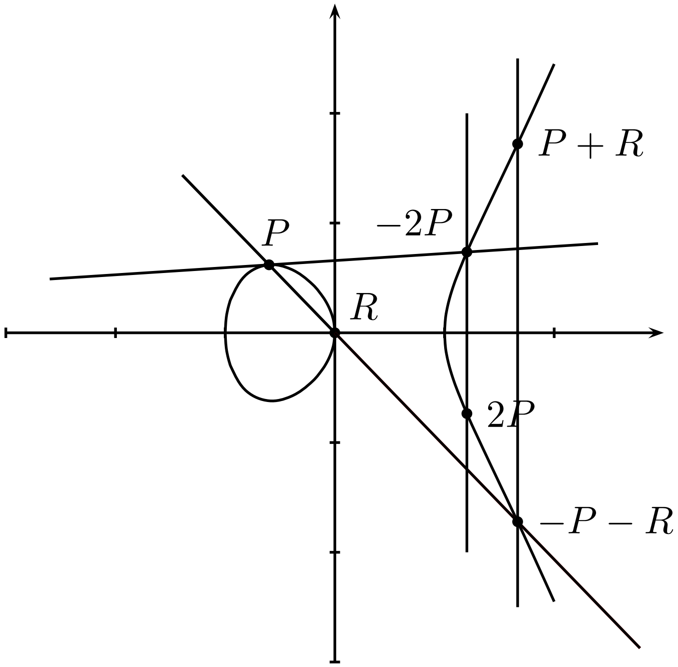
$$\begin{aligned} y_{-P-R} &= \lambda x_{-P-R} + \mu \\ &= \lambda x_{-P-R} + y_P - \lambda x_P \\ &= \lambda(x_{-P-R} - x_P) + y_P \end{aligned}$$

Point $P + R$ has the same $x$-coordinate but negative $y$-coordinate:

$$x_{P+R} = \lambda^2 - x_P - x_R, \quad y_{P+R} = \lambda(x_P - x_{-P-R}) - y_P$$

# Group Law ($q$ odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$




In general, for $(x_P, y_P) \neq (x_R, -y_R)$:

$$\begin{aligned}(x_P, y_P) + (x_R, y_R) &= \\ &= (x_{P+R}, y_{P+R}) = \\ &= (\lambda^2 - x_P - x_R, \lambda(x_P - x_{P+R}) - y_P),\end{aligned}$$

where

$$\lambda = \begin{cases} (y_R - y_P)/(x_R - x_P) & \text{if } x_P \neq x_R, \\ (3x_P^2 + a_4)/(2y_P) & \text{else.} \end{cases}$$

$\Rightarrow$ Addition and Doubling need
1 I, 2M, 1S and 1 I, 2M, 2S, respectively

# Weierstraß equation

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)}, \;\; h, f \in \mathbb{F}_q[x].$$

- Negative of $P = (x_P, y_P)$ is given by $-P = (x_P, -y_P - h(x_P))$.
- $(x_P, y_P) + (x_R, y_R) = (x_3, y_3) =$ $= (\lambda^2 + a_1\lambda - a_2 - x_P - x_R, \lambda(x_P - x_3) - y_P - a_1x_3 - a_3)$, where

$$\lambda = \begin{cases} (y_R - y_P)/(x_R - x_P) & \text{if } x_P \neq x_R, \\ \frac{3x_P^2+2a_2x_P+a_4-a_1y_P}{2y_P+a_Px_P+a_3} & \text{else.} \end{cases}$$

# Number of points

In cryptography we usually consider elliptic curves over finite fields $\mathbb{F}_q$.

Then the number of points is also finite, a bound is given by Hasse's theorem:

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

with

$$|t| \leq 2\sqrt{q}.$$

$t$ is called the trace of $E$.

Each point has finite order dividing $\#E(\mathbb{F}_q)$. Due to the Pohlig-Hellman attack we want to work in (sub-)groups of prime order $\ell$.

# Divisor class groups

## (Arithmetic on hyperelliptic curves)

# Example: Hyperelliptic Curves

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

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

$h(x), f(x) \in \mathbb{F}_q[x]$, $f$ monic, $\deg f = 2g + 1, \deg h \leq g$
non singular, i. e. not both partial derivatives

$$(2y + h(x) \text{ and } h'(x)y - f'(x))$$

vanish in any in $(a, b) \in C/\overline{\mathbb{F}_q}$

# Examples

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

$$y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6$$

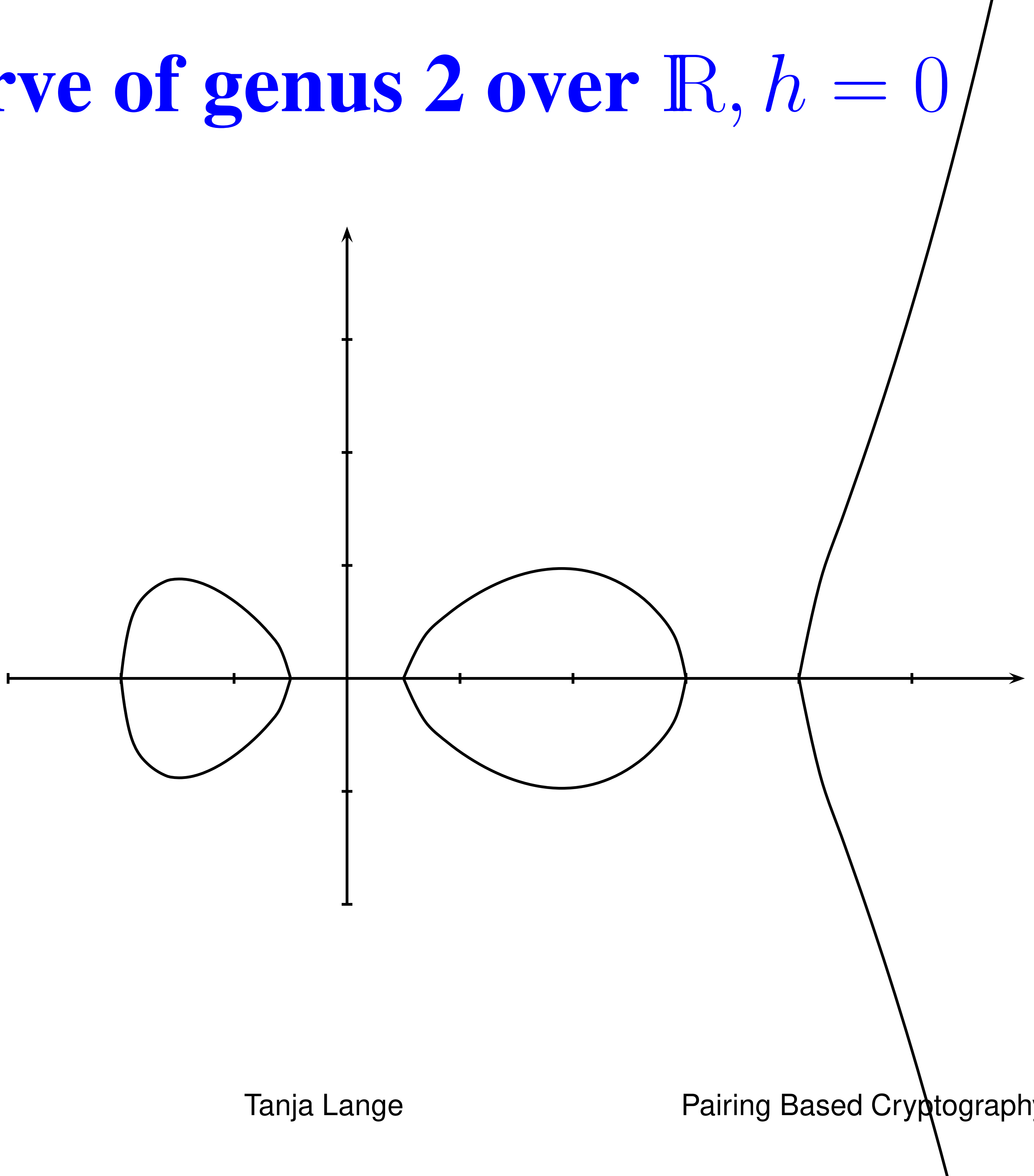
is considered as curve of genus one.

Curve of genus $2$ over field of odd characteristic

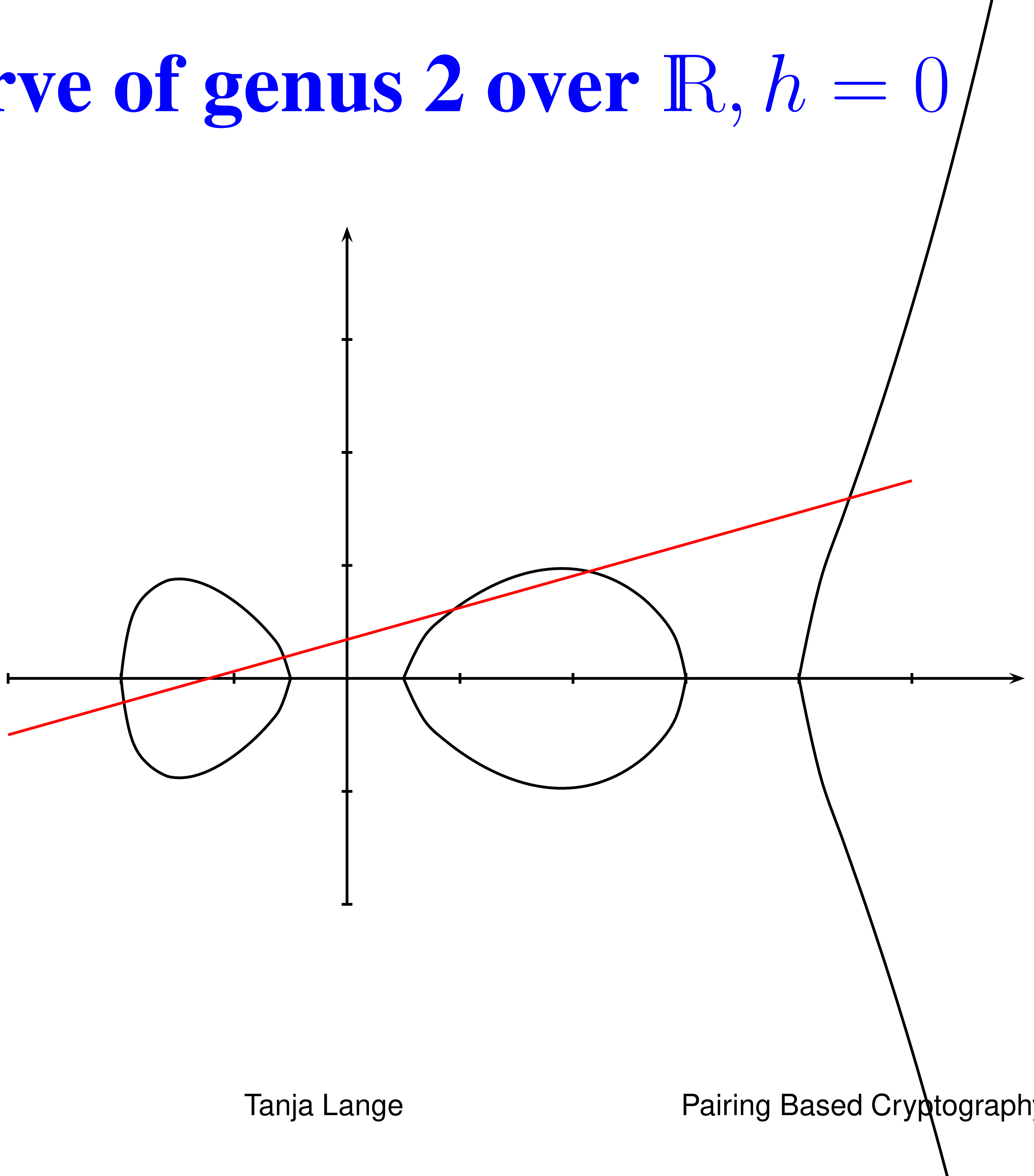
$$y^2 = x^5 + f_3 x^3 + f_2 x^2 + f_1 x + f_0,$$

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

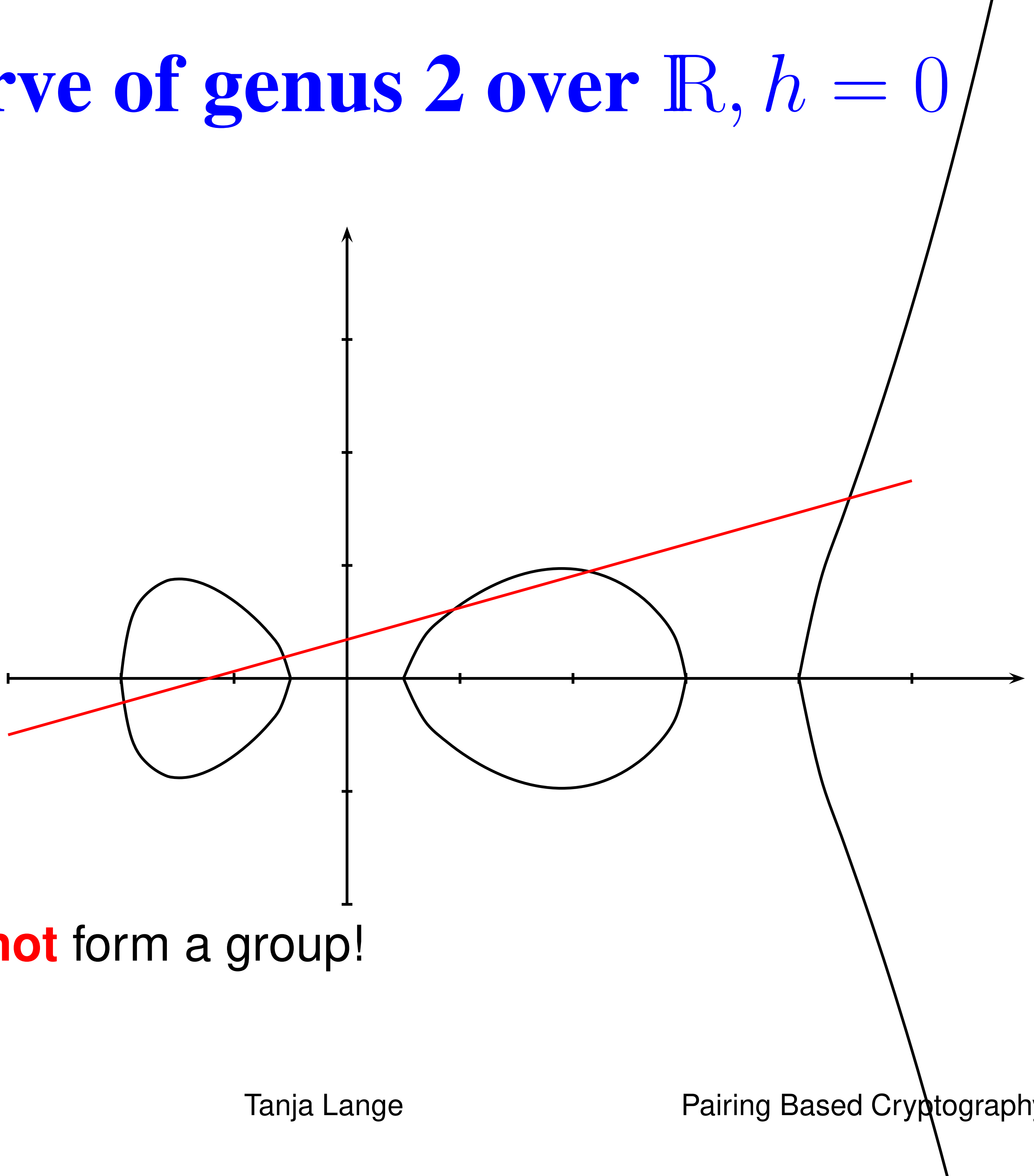
# Curve of genus 2 over $\mathbb{R}$, $h = 0$



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



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



points do **not** form a group!

# Group

Use Divisors, i. e. finite sums of points (elements of the free abelian group), of degree zero

$$\sum_{P \in C(\overline{\mathbb{F}_q})} n_P P, \; n_P \in \mathbb{Z}$$

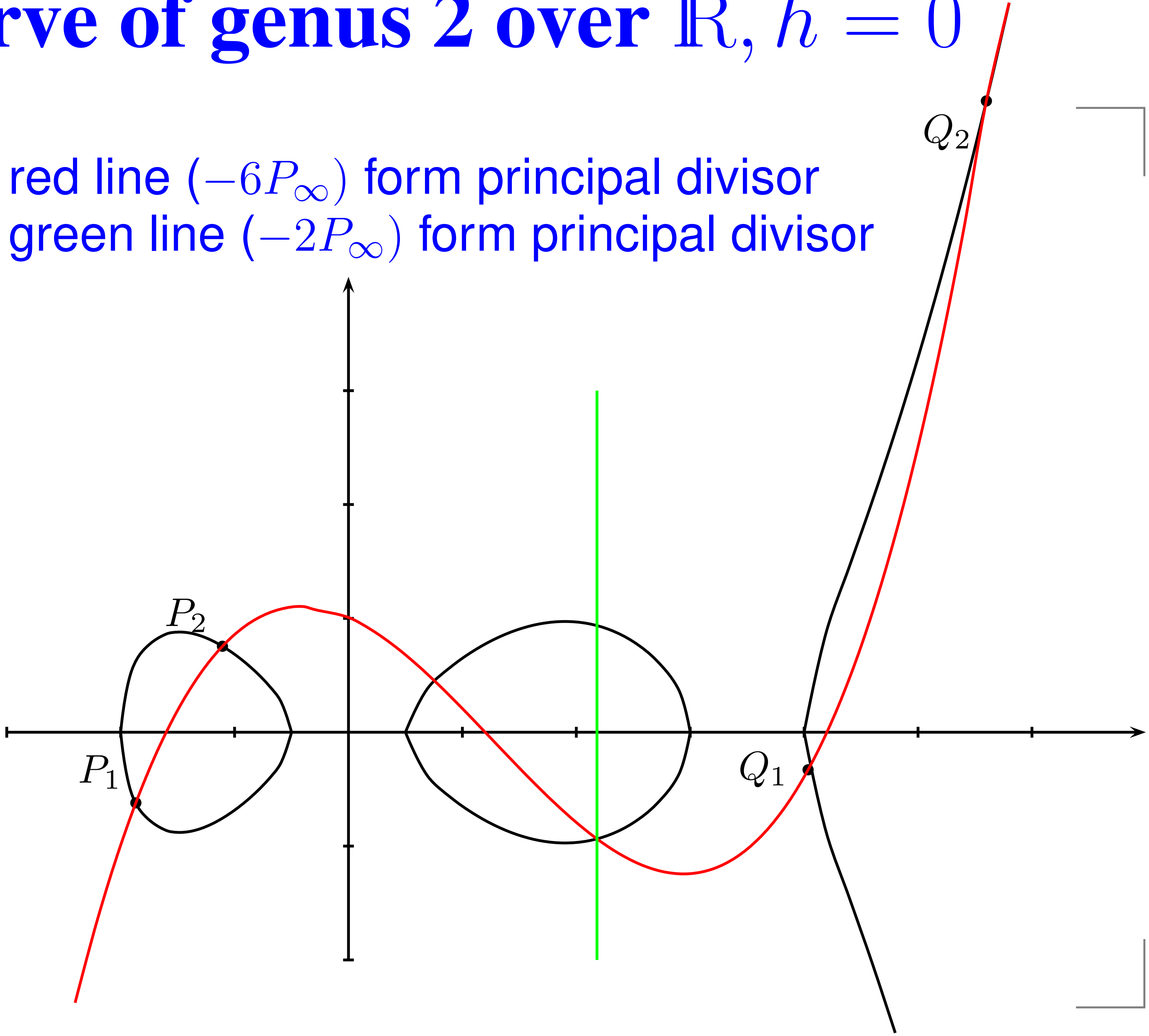
with $\sum_{P \in C(\overline{\mathbb{F}_q})} n_P = 0$ a $n_P = 0$ for almost all $P$.
One associates the divisor

$$\operatorname{div}(F) = \sum_{P \in C(\overline{\mathbb{F}_q})} v_P(F) P$$

to the function $F \in \mathbb{F}_q(C)$, where $v_P$ is a valuation in the point $P$. Such divisors are called principal divisors $\text{Princ}_C$.
One can show that they have degree zero.

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

points on red line $(-6P_\infty)$ form principal divisor
points on green line $(-2P_\infty)$ form principal divisor



# Divisor class group

Consider the factor group of the group of divisors of degree zero $\mathrm{Div}_C^0$ modulo the principal divisors. This way one constructs the divisor class group of degree zero.

$$\mathrm{Pic}_C^0 = \mathrm{Div}_C^0/\mathrm{Princ}_C.$$

The $\mathbb{F}_q$-rational group elements $\mathrm{Pic}_C^0(\mathbb{F}_q)$ are those which remain fixed under $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$.

This construction provides an isomorphism between $\mathrm{Pic}_C^0(\mathbb{F}_q)$ and the $\mathbb{F}_q$-rational points of the Jacobian of $C$.

# Representation of group elements

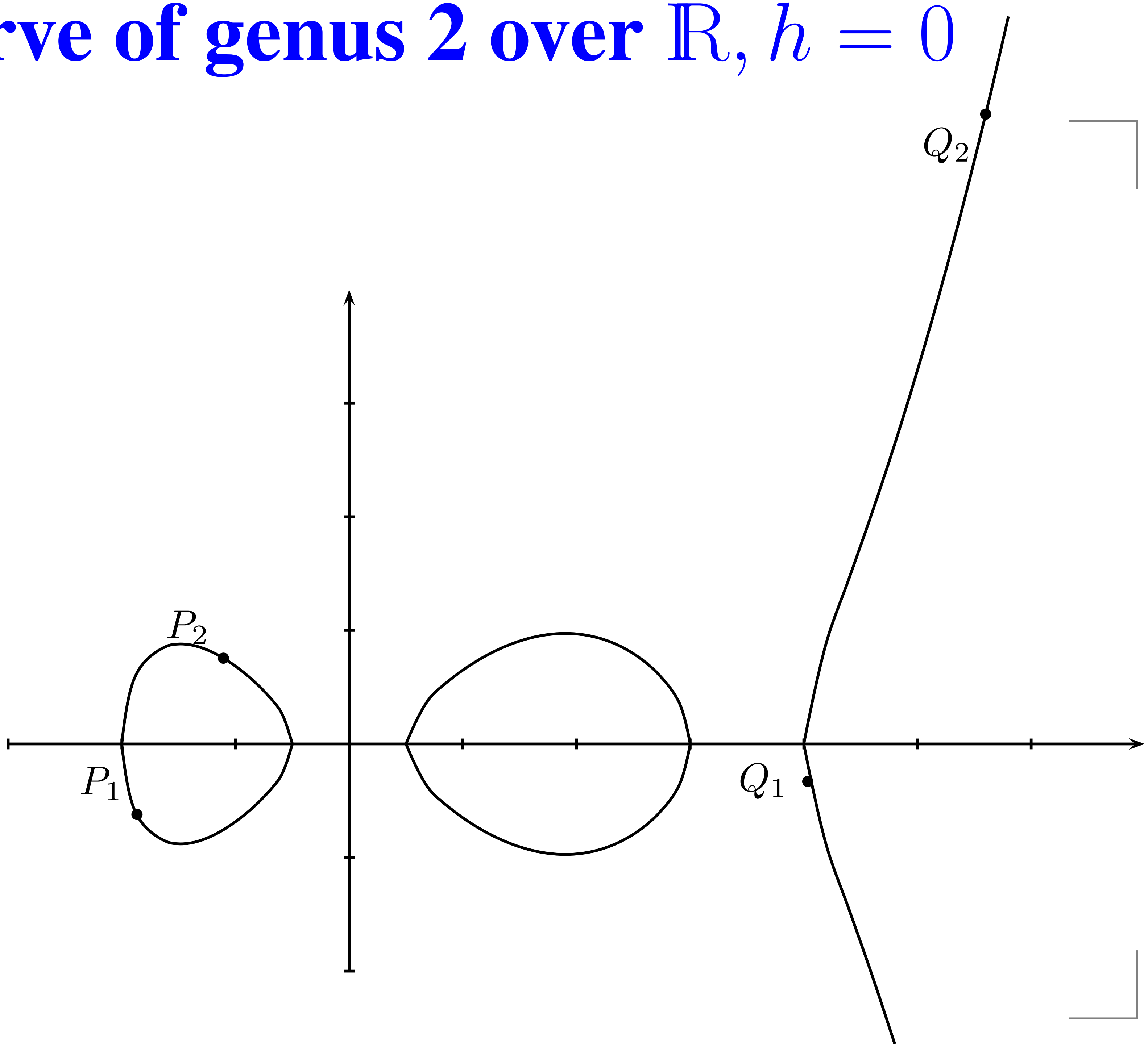
General:
Riemann-Roch allows to find a unique reduced representation by means of a divisor of degree zero with $m \leq g$

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

and $P_i \neq -P_j$ for $i \neq j$.

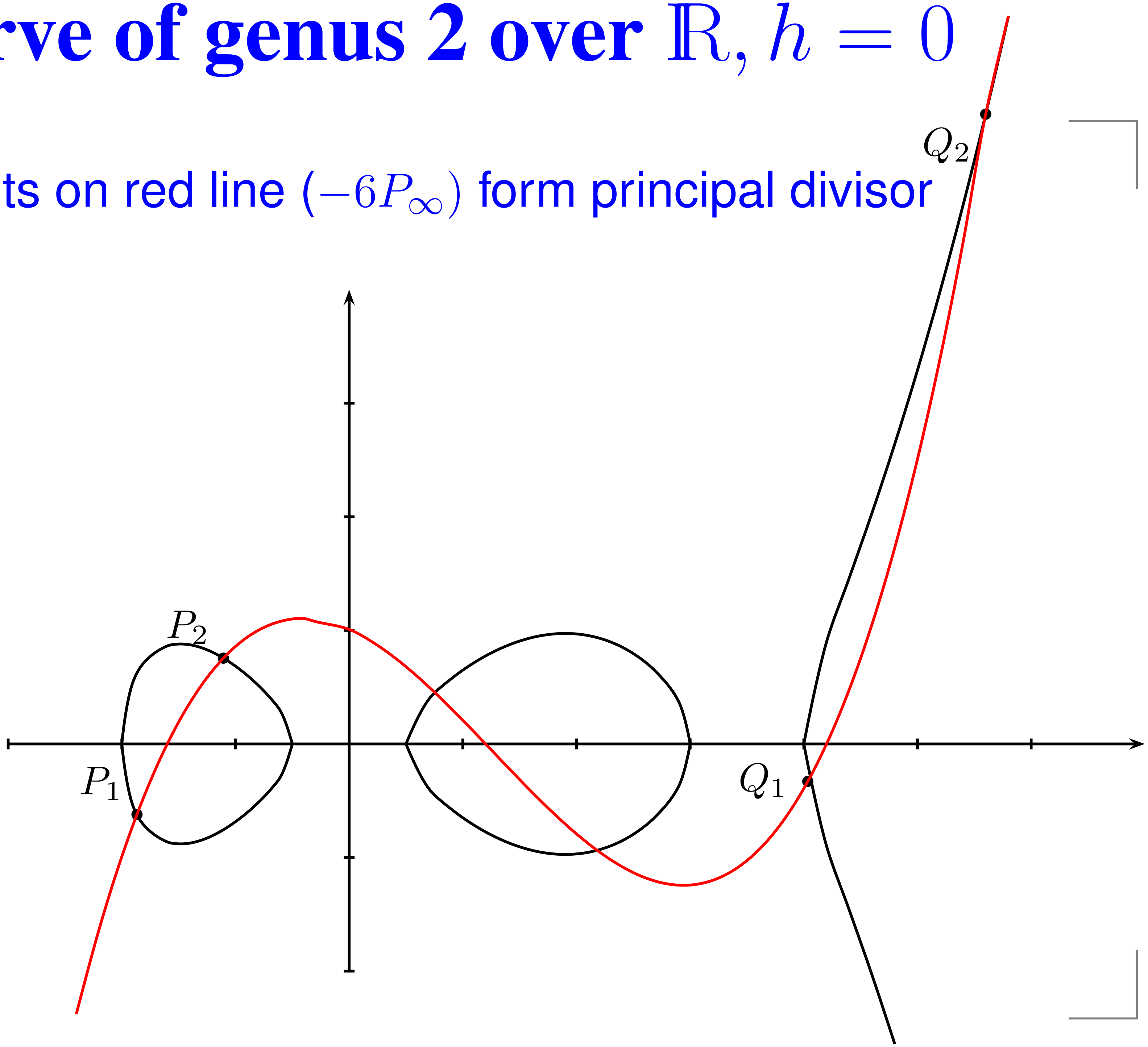
If $\bar{D}$ is defined over $\mathbb{F}_q$, the extension degree of the field of definition of the $P_i$ is bounded, e. g. at most $2$ for $g = 2$.

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



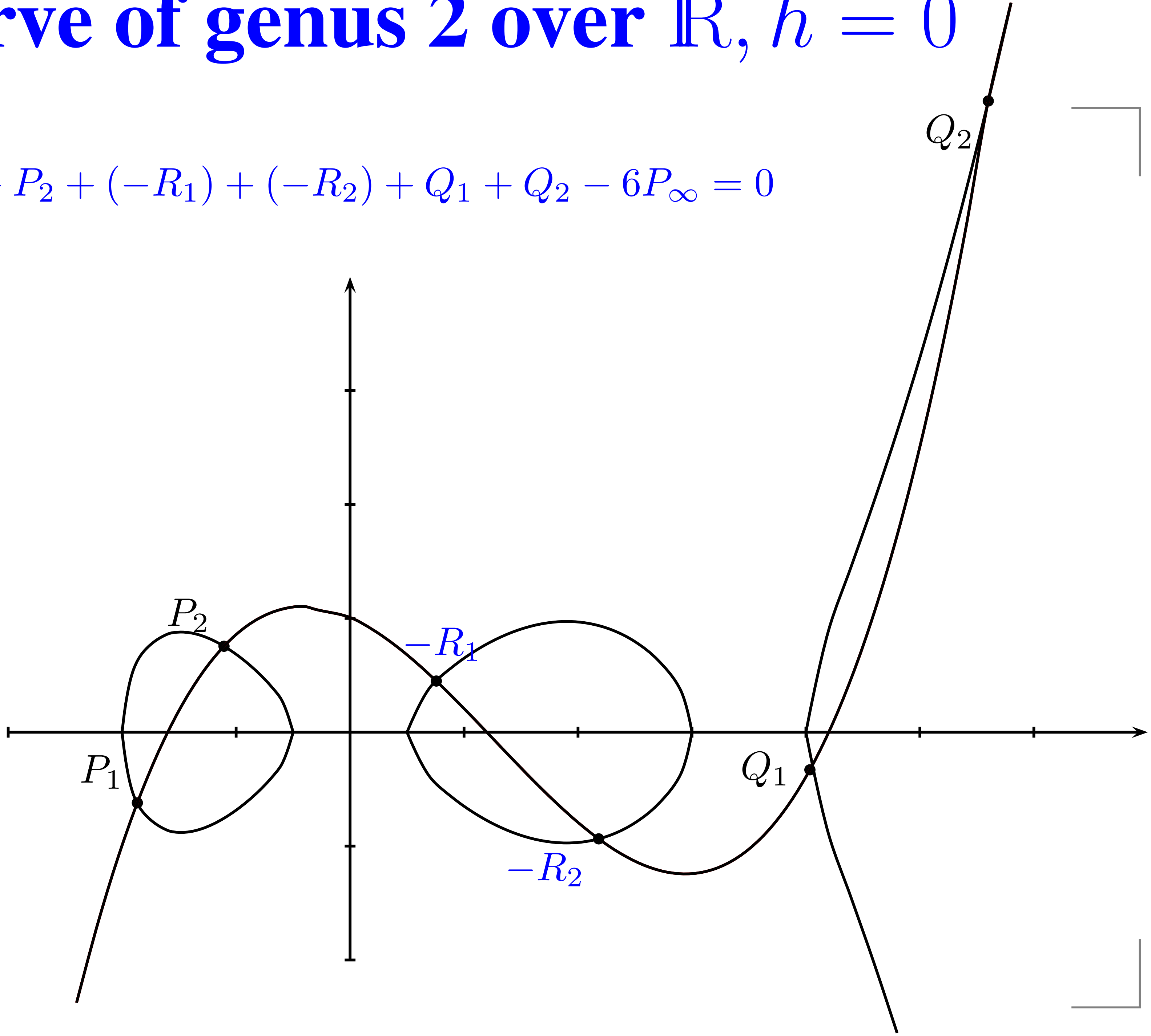
# Curve of genus 2 over $\mathbb{R}$, $h = 0$

points on red line $(-6P_\infty)$ form principal divisor



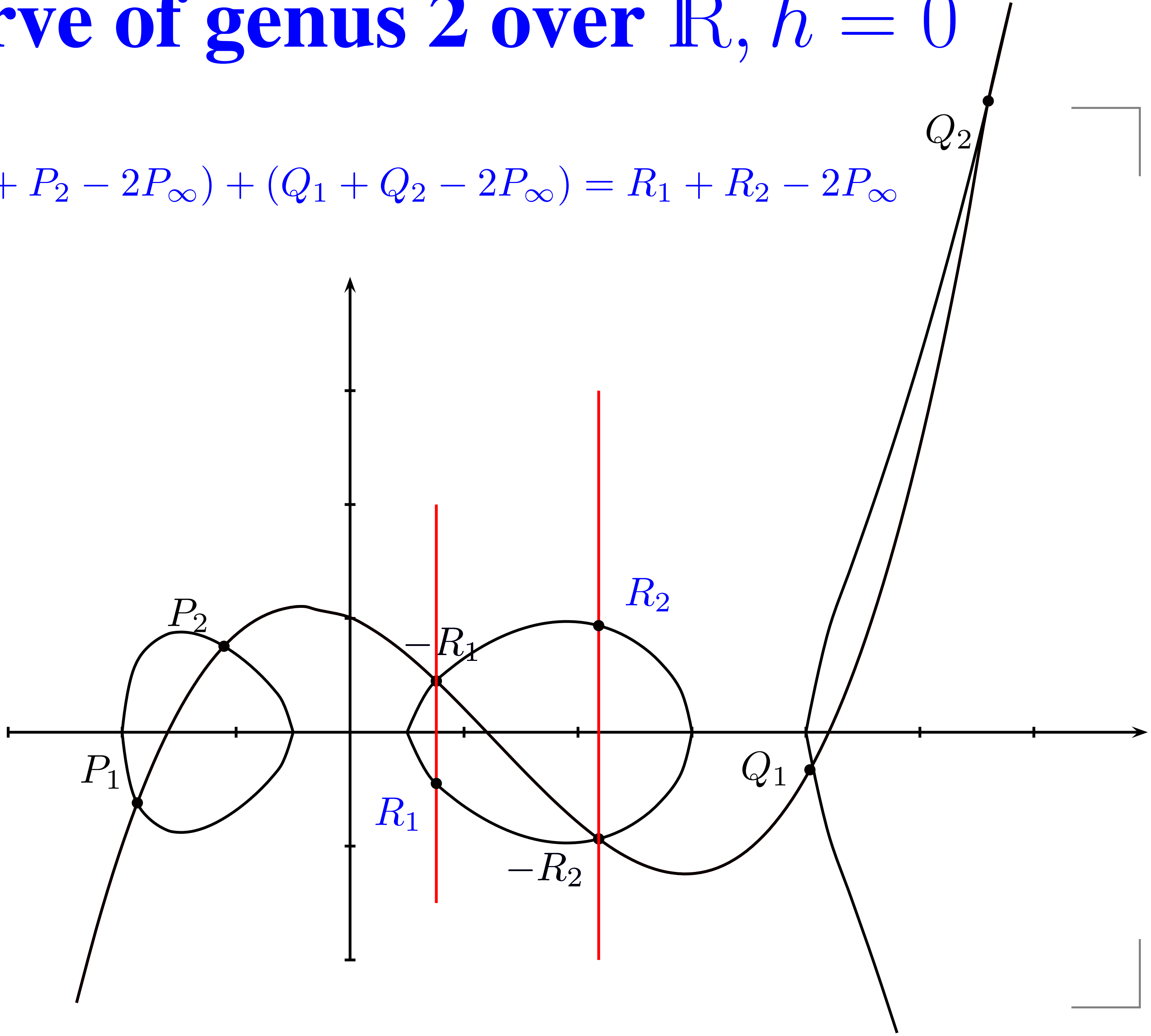
# Curve of genus 2 over $\mathbb{R}$, $h = 0$

$$P_1 + P_2 + (-R_1) + (-R_2) + Q_1 + Q_2 - 6P_\infty = 0$$



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

$$(P_1 + P_2 - 2P_\infty) + (Q_1 + Q_2 - 2P_\infty) = R_1 + R_2 - 2P_\infty$$



# Representation – elliptic curves

In the introduction we computed explicitly, that there is always a third point on a non-vertical line.

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

The isomorphism

$$\mathrm{Pic}^0_E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k}), \qquad \begin{aligned} P - P_\infty &\mapsto P \\ 0 &\mapsto P_\infty \end{aligned}$$

shows that the above construction gives a group on the points of $E$ together with the point at infinity.

# Pairings

# Prerequisites

We want to define pairings

$$G_1 \times G_1' \to G$$

preserving the group structure.

The pairings we use map to the multiplicative group of a finite extension field $\mathbb{F}_{q^k}$. To embed the points of order $\ell$ the embedding degree $k$ has to be chosen large enough so that the $\ell$-th roots of unity are in $\mathbb{F}_{q^k}^*$.

So choose

$$k \text{ minimal with } \ell \mid q^k - 1.$$

# Tate-Lichtenbaum pairing I

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

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

Let $\bar{D}_2 \in \mathrm{Pic}^0_C(\mathbb{F}_{q^k})$ 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

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

as $\ell$-folds are in the kernel of $T_\ell$.
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 $\mathbb{F}_{q^k}$ 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

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

to define pairing on points $T_\ell(P, Q)$, with

$$D_1 = P - P_\infty, D_2 = (Q + R) - R$$

for some $R$.

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

Often

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

# Miller's algorithm

In: $\ell = \sum_{i=0}^{n-1} \ell_i 2^i$, $P, Q+R, R$
Out: $T_\ell(P,Q)$

1. $T \leftarrow P$, $F \leftarrow 1$
2. for $i = n-2$ downto $0$ do
   (a) Calculate lines $l$ and $v$ in doubling
   $T \leftarrow 2T$
   $F \leftarrow F^2 \cdot l(Q+R)v(R)/(l(R)v(Q+R))$
   (b) if $\ell_i = 1$ then
   Calculate lines $l$ and $v$ in addition $T+P$
   $T \leftarrow T+P$
   $F \leftarrow F \cdot l(Q+R)v(R)/(l(R)v(Q+R))$
3. return $F$

# Weil pairing

For an elliptic curve $E$ define

$$\begin{aligned} W_\ell : E(\overline{\mathbb{F}}_q)[\ell] \times E(\overline{\mathbb{F}}_q)[\ell] &\rightarrow \mu_\ell \\ (P,Q) &\mapsto \frac{F_{P-P_\infty}(D_Q)}{F_{Q-P_\infty}(D_P)} \end{aligned}$$

where $\mu_\ell$ is the multiplicative groups of the $\ell$-th roots of unity in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$.
Obviously, $W_\ell(P,P) = 1$.

Weil pairings can be seen as two-fold application of the Tate-Lichtenbaum pairing, note $Q \in E(\mathbb{F}_{q^k})$.

Needs full group of order $\ell$ in $E(\mathbb{F}_{q^k})$, if $k = 1$ then the Weil pairing is trivial & one needs to use larger field.

# Efficient computation

# $k$ minimal

Observation:
$k$ is minimal with $\ell \mid q^k - 1$, so final exponentiation $T_\ell(\bar{D}_1, \bar{D}_2)^{(q^k-1)/\ell}$ removes all terms from subfields.

- Choose $R \in E(\mathbb{F}_q)$, computation of $l(R)$ and $v(R)$ not needed.
- Choose $R = P_\infty$,

$$\tilde{T}_\ell(P, Q) = F_{P-P_\infty}(Q)^{(q^k-1)/\ell}.$$

- If protocol allows, choose $Q = (x_Q, y_Q) \in \mathbb{F}_{q^k}$ with $x$ in subfield, this avoids computation of $v(Q)$. This means no extra division!

# Improvements to Miller

Observation:
Let $N = c\ell$ for some $c$, then

$$\tilde{T}_\ell(P,Q) = T_\ell(P,Q)^{(q^k-1)/\ell} = T_N(P,Q)^{(q^k-1)/N}.$$

- Other addition chains can be used in Miller's algorithm, e.g. NAF.
  Other bases might be good depending on characteristic of the field.
- Use multiple $N$ with low Hamming weight (in $p$-adic representation).
  For supersingular curves choosing $N$ as number of points gives fast final exponentiation.

# Special curves

Duursma-Lee and Barreto-Galbraith-O hEigeartaigh-Scott obtain further speed-up by choosing supersingular curves of genus $(p-1)/2$ over $\mathbb{F}_{p^r}$.

Main ideas are to use $p$ as basis in addition chain $\Rightarrow$ much shorter chain and take into account that each order divides $p^r + 1$.

Key words are “eta-pairing” and “eta-T-pairing”.

# Supersingular and ordinary

# Definition

Let $E$ be an elliptic curve defined over $\mathbb{F}_q, q = p^r$.
$E$ is supersingular if

- $E[p^s](\overline{\mathbb{F}}_q) = \{P_\infty\}$.
- $t \equiv 0 \bmod p$.
- $\mathrm{End}_E$ is order in quaternion algebra.

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

Example:

$$y^2 + y = x^3 + a_4x + a_6 \text{ over } \mathbb{F}_{2^r}$$

is supersingular, as a point of order $2$ would satisfy

$$y_P = y_P + 1$$

which is impossible.

# Distortion map I

For supersingular curves it is possible to find maps $\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^k})$ that map to a linearly independent subgroup, i.e.

$$T'_\ell(P,P) \neq 1 \text{ for } T'_\ell(P,P) = T_\ell(P, \phi(P)).$$

(This needs that there are independent endomorphisms, so no chance for ordinary curves).
Examples:

- $y^2 = x^3 + a_4 x$, for $p \equiv 3 \pmod 4$.
  Distortion map $(x,y) \mapsto (-x, iy)$ with $i^2 = -1$
- $y^2 = x^3 + a_6$, for $p \equiv 2 \pmod 3$.
  Distortion map $(x,y) \mapsto (jx, y)$ with $j^3 = 1, j \neq 1$,

In both cases, $\#E(\mathbb{F}_p) = p+1$, $k = 2$.

# Distortion maps II

- Over $\mathbb{F}_{2^d}$ consider
$$y^2 + y = x^3 + x + a_6, \text{ with } a_6 = 0 \text{ or } 1$$
and distortion map
$$(x, y) \mapsto (x+s^2, y+sx+t), \; s, t \in \mathbb{F}_{2^{4d}}, \; s^4+s = 0, \; t^2+t+s^6+s^2 = 0.$$
$$\#E(\mathbb{F}_{2^d}) = 2^d + 1 \pm 2^{(d+1)/2}, \; k = 4.$$
- Over $\mathbb{F}_{3^d}$ consider
$$y^2 = x^3 + x + a_6, \text{ with } a_6 = \pm 1$$
and distortion map
$$(x, y) \mapsto (-x + s, iy) \text{ with } s^3 + 2s + 2a_6 = 0 \text{ and } i^2 = -1.$$
$$\#E(\mathbb{F}_{3^d}) = 3^d + 1 \pm 3^{(d+1)/2}, \; k = 6.$$

# Application of distortion maps

- Distortion maps allow to state the protocols as using bilinear map
$$G_1 \times G_1 \to G.$$
- Scalar multiplications of input point can be performed over $\mathbb{F}_q$ and then mapped into $E(\mathbb{F}_{q^k})$, this saves computation time
$\Rightarrow$ obvious computational savings in the above protocols.
- Can be used to map on points with $x$-coordinate in subfield.
- Systems are easier to state.
- Really short signatures (see next slide).

# Short signatures

Boneh, Lynn, and Shacham, Asiacrypt 2001

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

User secret key $s$, public key $[s]P$.

Signature of message $m$:
Compute and send $S = [s]H(m)$.

Verification:
Check if

$$e([s]P, H(m)) = e(P, S).$$

Point compression to the $x$-coordinate achieves signatures given by one field element, i.e. of half the length of ECDSA.

# Embedding degree

# Embedding degrees I

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

Hasse's Theorem states $|t| \leq 2\sqrt{q}$ and $E$ supersingular implies $t \equiv 0 \bmod p$, so $t = 0$ and

$$|E(\mathbb{F}_p)| = p + 1.$$

Obviously

$$(p+1) \mid p^2 - 1 = (p+1)(p-1)$$

so $k \leq 2$ for supersingular curves over prime fields.

# Parameter sizes

For DLP in groups one has square-root attacks, for finite fields index calculus methods are more efficient. A common requirement is

- $\#E(\mathbb{F}_q) \sim q$: 160 bits
- $q^k$: 1024 bits
- optimal embedding degree would be

$$k = 1024/160 = 6.4$$

However, $6$ is only attained for small characteristic and there Coppersmith methods require larger fields, cf. Page, Smart, and Vercauteren.
Difference between sizes grows $\Rightarrow$ larger $k$ becomes optimal.

# Embedding degrees II

Let $E$ be supersingular.
Menezes, Okamoto, and Vanstone show:

- in characteristic $2$ we have $k \leq 4$,
- in characteristic $3$ we have $k \leq 6$,
- over prime fields $\mathbb{F}_p$ with $p \geq 5$ we have $k \leq 2$,

and these bounds are attained.

Now or soon, larger $k$ become necessary, no chance with supersingular elliptic curves, little hope for larger genus hyperelliptic.

# MNT curves

# MNT curves I

Find ordinary curves with small embedding degree! Thus force

$$q + 1 - t \equiv 0 \pmod{\ell} \text{ and } q^k - 1 \equiv 0 \pmod{\ell}.$$

History:

- Original proposal by Miyaji, Nakabayashi, and Takano.
- Dupont, Enge, Morain: small $k$ by CM
- More examples:
  Barreto, Lynn, Scott; Brezing, Weng;
  Curves for $k = 3, 4$ and $6$.
- Generalization to co-factors, $k = 5, 10, 12$
  Galbraith, McKee, Valença.
- Family of curves with $k = 12$
  Barreto and Naehrig.

# MNT curves II

To find families of curves consider $k$-th cyclotomic polynomials $\Phi_k \mid x^k - 1$ for small $k$, here $\deg(\Phi_k) = 2$.

$$\begin{aligned} \Phi_3(x) &= x^2 + x + 1, \\ \Phi_4(x) &= x^2 + 1, \\ \Phi_6(x) &= x^2 - x + 1. \end{aligned}$$

Use CM-method but fix the ground field $\mathbb{F}_q$ and vary the discriminant of the quadratic number field. CM method allows to find curve given base field $\mathbb{F}_q$ and trace $t$ by trying to solve the CM-equation

$$Dv^2 = 4q - t^2$$

for sufficiently small values of $D$.

# MNT curves – computation

$$Dv^2 = 4c\frac{\Phi_k(t-1)}{c'} - (t-2)^2$$

using $q = c\ell + t - 1$ and $\Phi_k(t-1) = c'\ell$.
Use $\Phi_k$ and put $n_3 = 2c + c'$, $n_4 = c'$, $n_6 = -2c + c'$,
$m = 4c - c'$, $r = c'mD$, $y = m(t-1) + n_k$ and $f_k = n_k^2 - m^2$,
the CM-equation simplifies to the generalized Pell equation

$$y^2 - rv^2 = f_k.$$

For each solution, we must check that

- $t = \frac{y-n_k}{m} + 1$ is an integer
- $\ell = \frac{\Phi_k(t-1)}{c'}$ is prime, and
- $q = c\ell + t - 1$ is prime

# Comparison

# Supersingular vs. ordinary

Supersingular:

- pro: known, speed ups by choosing $N = c\ell$, eta-T-pairing, distortion maps
- con: only small $k$, far too large field size for prime fields, small number of curves

Ordinary:

- pro: can be used over prime fields, more and larger embedding degrees possible, more (but also finite) choice
- con: no distortion maps, no reason why good multiple $N$ should exist, no loop-shortening

# Outlook

Pairings are a very active area of research, e.g. on the following tasks

- find more protocols / solve posed problems,
- speed up the computation,
- find more MNT curves,
- consider other curves, e.g. hyperelliptic curves.

Great collection at

P. S. L. M. Barreto, “The Pairing-Based Crypto Lounge”

`http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html`

- Break system???

# Literature

- P. S. Barreto, S. Galbraith, C. O hEigeartaigh, M. Scott
  "Efficient Pairing Computation on Supersingular Abelian Varieties"
- R. Dutta, R. Barua, and P. Sakar
  "Pairing-based cryptography: A survey"
- D. Hankerson and A. J. Menezes and S. A. Vanstone
  "Guide to elliptic curve cryptography"
- Chapter in
  "Advances in Elliptic Curve Cryptography",
  by I. F. Blake, G. Seroussi, and N. P. Smart (Editors)
- Chapters in
  "Handbook of Elliptic and Hyperelliptic Curve Cryptography", by H. Cohen and G. Frey (Editors)