Efficient arithmetic on (hyper-)elliptic curves over finite fields

Tanja Lange

Department of Mathematics

Technical University of Denmark

t.lange@mat.dtu-dk

15.03.2005

Overview

- Arithmetic on elliptic curves
- Arithmetic on hyperelliptic curves
- Special case of characteristic two

Arithmetic on elliptic curves

Elliptic curve

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

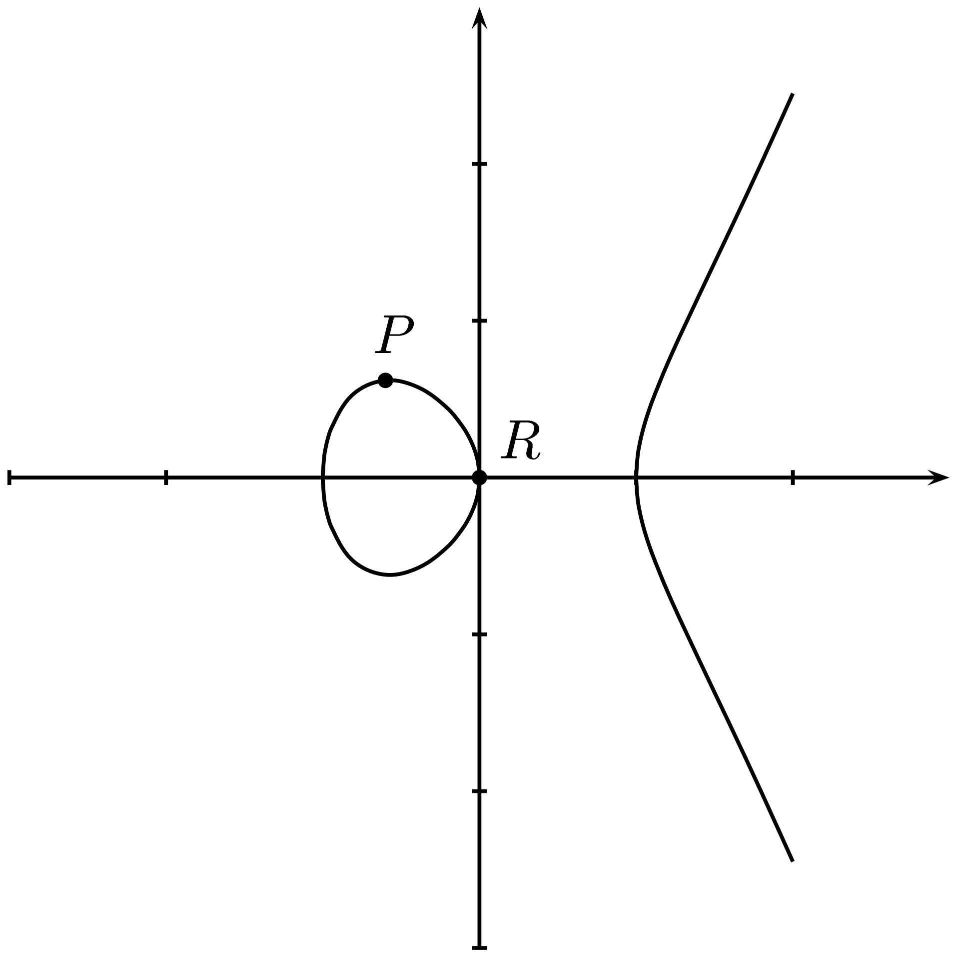
Group: $E(\mathbb{F}_q) = \{\, (x, y) \in \mathbb{F}_q^2 \; : \; y^2 + h(x)y = f(x) \,\} \cup \{\, P_\infty \,\}$

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

$$\begin{aligned} y^2 &= f(x) && q \text{ odd}, \\ y^2 + xy &= x^3 + ax^2 + b && q = 2^r, \text{ curve non-supersingular} \end{aligned}$$

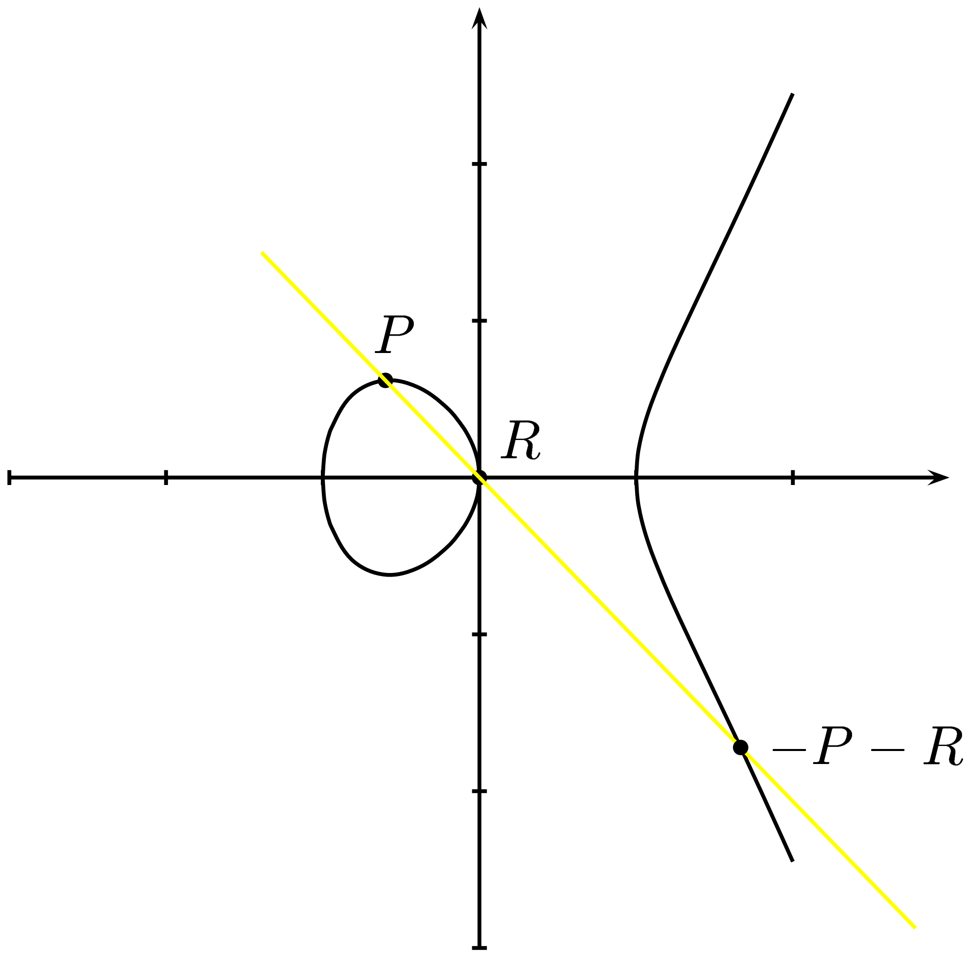
Group Law in $\boldsymbol{E(\mathbb{R}), h = 0}$

$y^2 = x^3 - x$



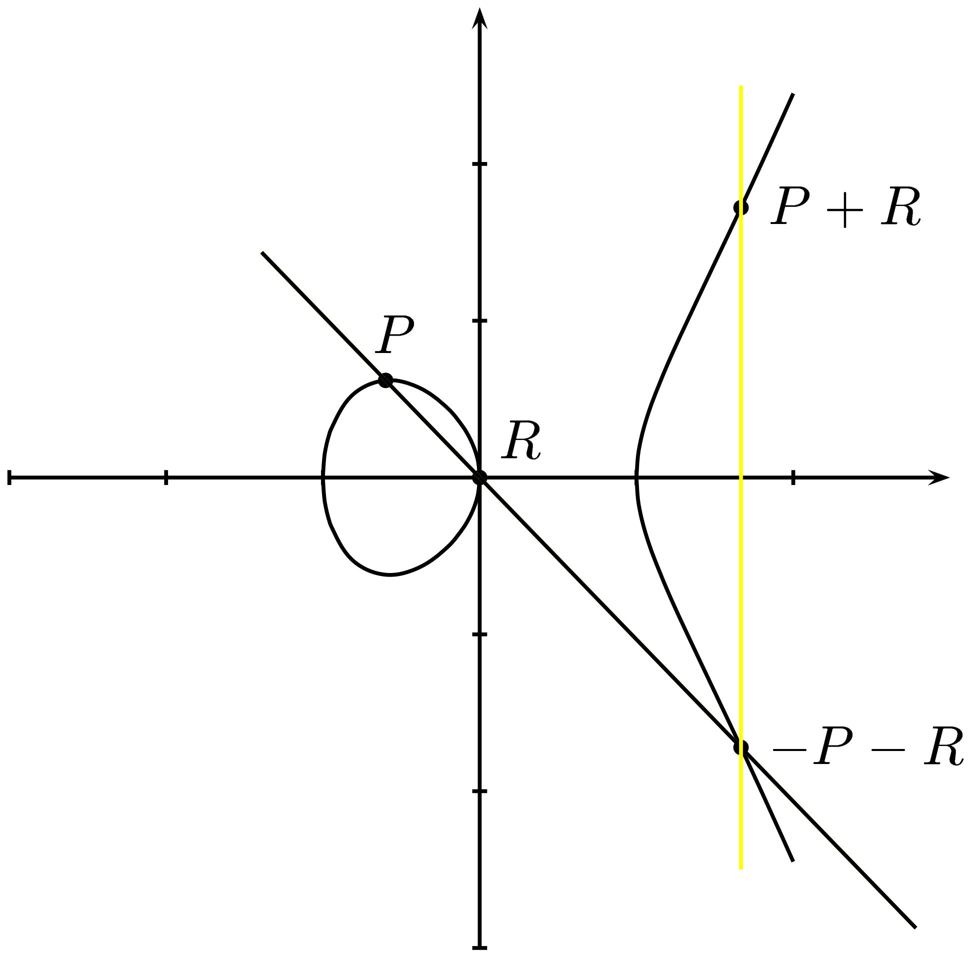
Group Law in $\boldsymbol{E(\mathbb{R}), h = 0}$

$y^2 = x^3 - x$



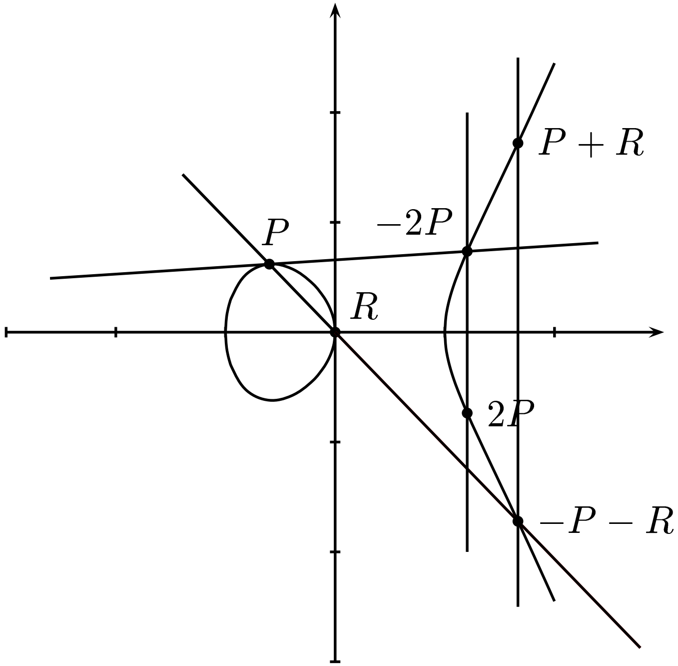
Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



Group Law (q odd)

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



for $(x_1, y_1) \neq (x_2, -y_2)$:

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &= \\ &= (x_3, y_3) = \\ &= (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),\end{aligned}$$

where

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } x_1 \neq x_2, \\ (3x_1^2 + a_4)/(2y_1) & \text{else.} \end{cases}$$

$\Rightarrow$ Addition and Doubling differ considerably.

1 I, 2M, 1S vs. 1 I, 2M, 2S

Projective Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P \oplus Q = (X_3 : Y_3 : Z_3)$
on $E : Y^2Z = X^3 + a_4XZ^2 + a_6$

Addition: $P \neq \pm Q$	Doubling $P = Q \neq -P$
$A = Y_2Z_1 - Y_1Z_2, B = X_2Z_1 - X_1Z_2,$	$A = a_4Z_1^2 + 3X_1^2, B = Y_1Z_1,$
$C = A^2Z_1Z_2 - B^3 - 2B^2X_1Z_2$	$C = X_1Y_1B, D = A^2 - 8C$
$X_3 = BC, Z_3 = B^3Z_1Z_2$	$X_3 = 2BD, Z_3 = 8B^3.$
$Y_3 = A(B^2X_1Z_2 - C) - B^3Y_1Z_2,$	$Y_3 = A(4C - D) - 8Y_1^2B^2$

No inversion is needed and the computation times are $12M + 2S$ for a general addition and $7M + 5S$ for a doubling.

Jacobian Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P \oplus Q = (X_3 : Y_3 : Z_3)$
on $Y^2 = X^3 + a_4 X Z^4 + a_6 Z^6$ by

Addition: $P \neq \pm Q$

$A = X_1 Z_2^2, B = X_2 Z_1^2, C = Y_1 Z_2^3,$

$D = Y_2 Z_1^3, E = B - A, F = D - C$

$X_3 = -E^3 - 2AE^2 + F^2, Z_3 = Z_1 Z_2 E,$

$Y_3 = -CE^3 + F(AE^2 - X_3),$

Doubling $P = Q \neq -P$

$A = 4X_1 Y_1^2, B = 3X_1^2 + a_4 Z_1^4$

$X_3 = -2A + B^2, Z_3 = 2Y_1 Z_1$

$Y_3 = -8Y_1^4 + B(A - X_3).$

No inversion is needed and the computation times are
$12M + 4S$ for a general addition and $4M + 6S$ for a doubling.

Different coordinate systems $y^2 = x^3 + ax + b$

system	points	correspondence
affine ($\mathcal{A}$)	(x, y)	
projective ($\mathcal{P}$)	(X, Y, Z)	$(X/Z, Y/Z)$
jacobian ($\mathcal{J}$)	(X, Y, Z)	$(X/Z^2, Y/Z^3)$
Chudnovsky jacobian ($\mathcal{J}^C$)	(X, Y, Z, Z^2, Z^3)	$(X/Z^2, Y/Z^3)$
modified jacobian ($\mathcal{J}^m$)	(X, Y, Z, aZ^4)	$(X/Z^2, Y/Z^3)$

system	addition			doubling		
affine ($\mathcal{A}$)	2M	1S	1I	2M	2S	1I
projective ($\mathcal{P}$)	12M	2S	–	7M	5S	–
jacobian ($\mathcal{J}$)	12M	4S	–	4M	6S	–
Chudnovsky jacobian ($\mathcal{J}^C$)	11M	3S	–	5M	6S	–
modified jacobian ($\mathcal{J}^m$)	13M	6S	–	4M	4S	–

Mixed coordinates

(Cohen, Miyaji, Ono, Asiacrypt '98)

affordable inversions:
precomputations in $\mathcal{A}$ (with Montgomery),
main doublings in $\mathcal{J}^m$,
final doublings $2\mathcal{J}^m = \mathcal{J}$,
additions $\mathcal{A} + \mathcal{J} = \mathcal{J}^m$

expensive inversions:
precomputations in $\mathcal{J}^C$,
main doublings in $\mathcal{J}^m$,
final doublings $2\mathcal{J}^m = \mathcal{J}$,

additions $\mathcal{J} + \mathcal{J}^C = \mathcal{J}^m$

Arithmetic on hyperelliptic curves

Hyperelliptische Kurven

Affine equation of hyperelliptic curve of genus g (with K-rational Weierstraß-point at infinity)

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

$h(x), f(x) \in K[x]$, 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 $(a, b) \in C/\overline{K}_q$

Examples

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

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

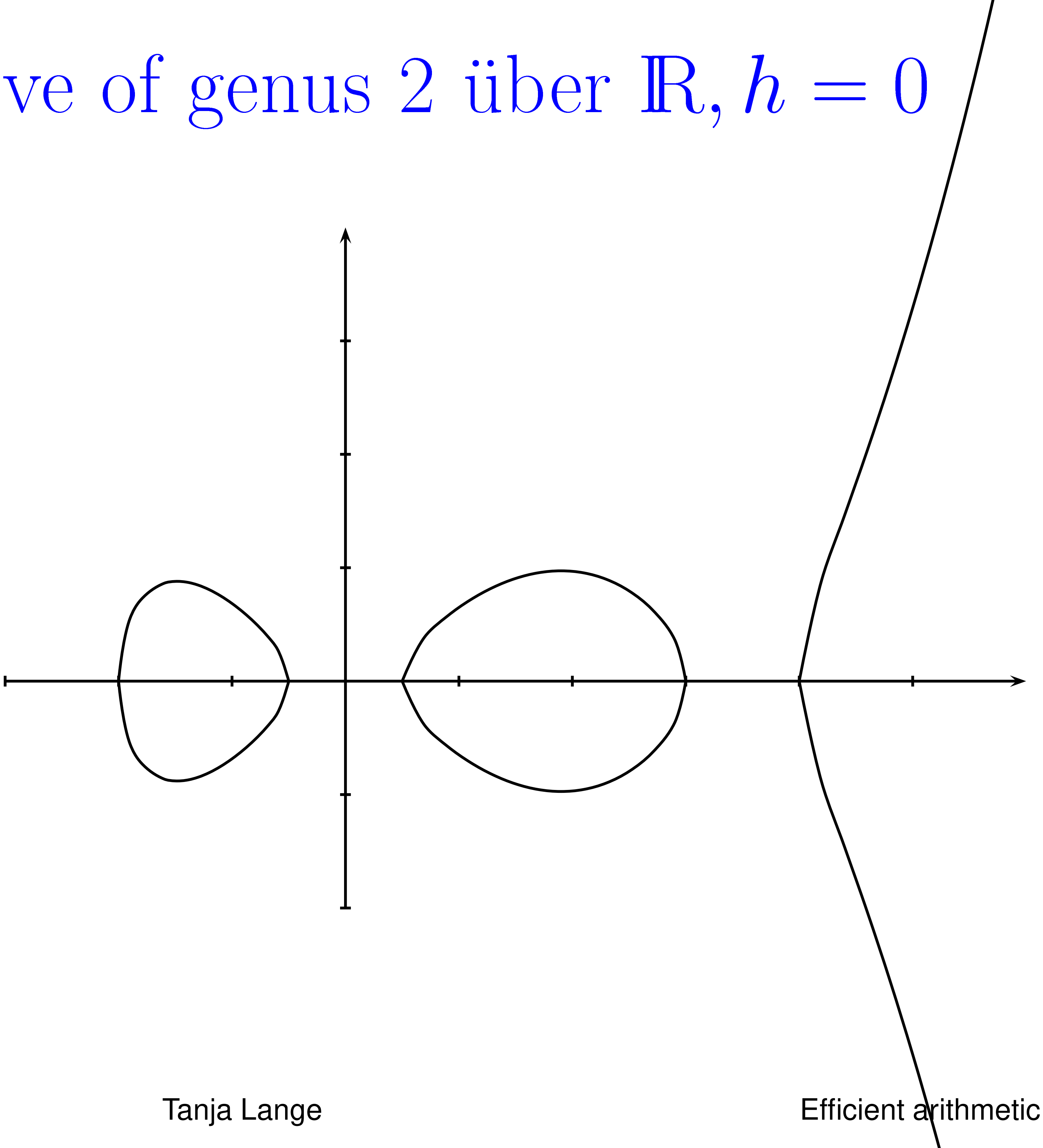
is considered as curve of genus one.

Curve of genus 2 over field of odd characteristic

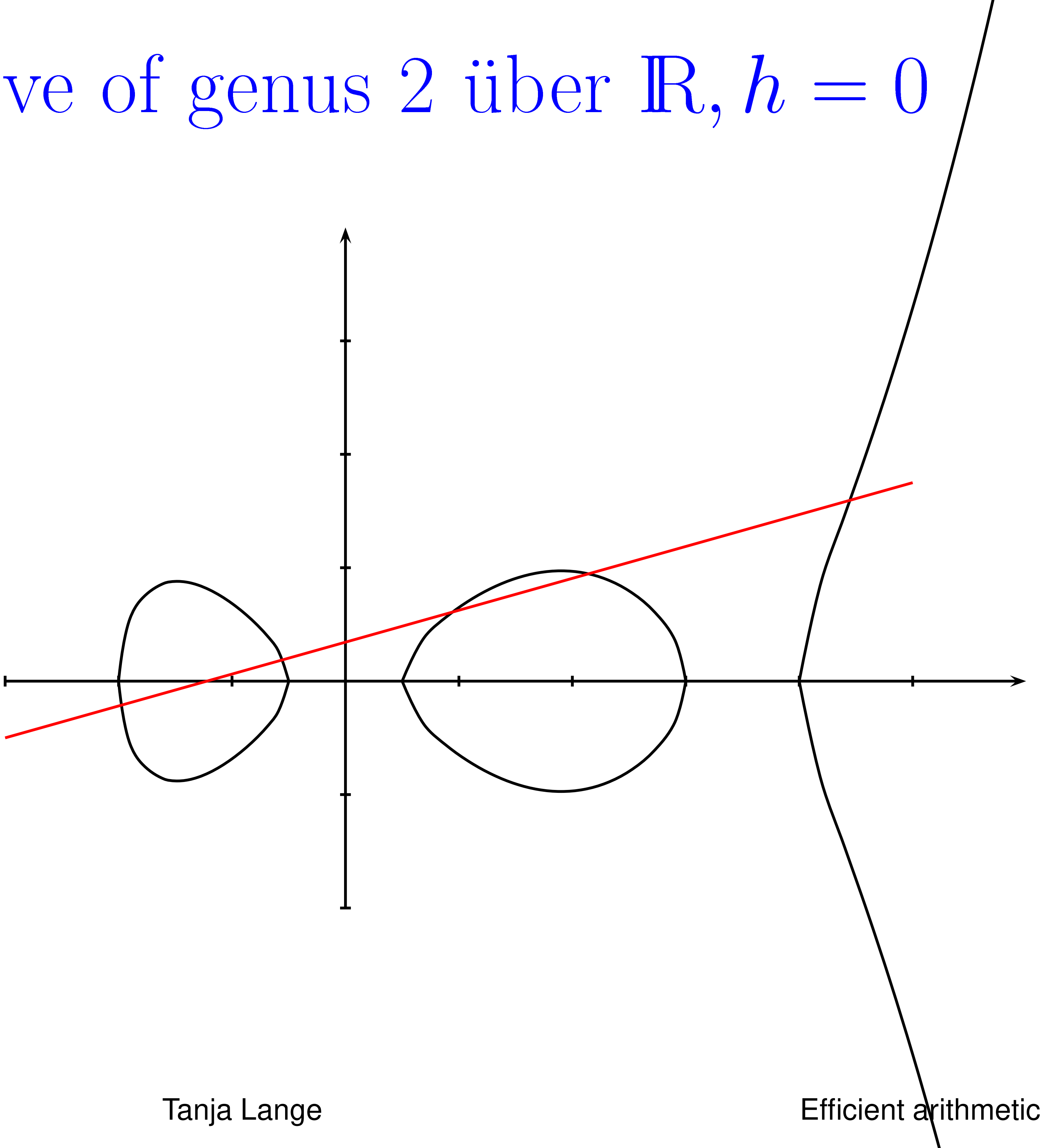
$$y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

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

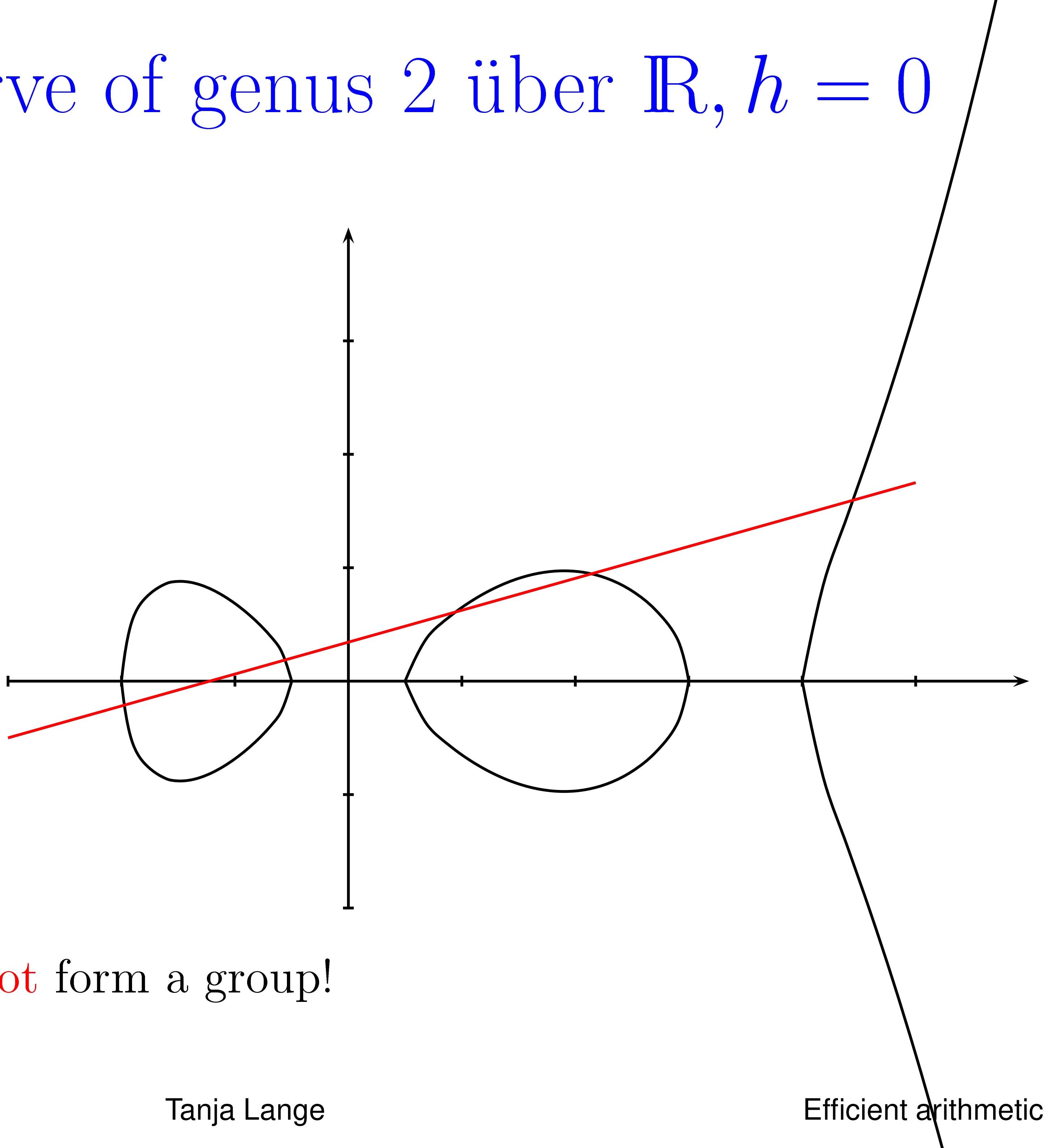
Curve of genus 2 über $\mathbb{R}, h = 0$



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



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



points do not form a group!

Group

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

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

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

$$\mathrm{div}(f) = \sum_{P \in C(\overline{K})} v_P(f) P$$

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

Divisor class group

Consider the factor group of the group of divisors of degree zero Div_C^0 modulo the principal divisors. This way one constructs the divisor class group of degree zero.

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

The K-rational group elements $\mathrm{Pic}_C^0(K)$ are those which remain fixed under $\mathrm{Gal}(\overline{K}/K)$.
This construction provides an isomorphism between $\mathrm{Pic}_C^0(K)$ and the K-rational points of the Jacobian of C.

Representation of group elements

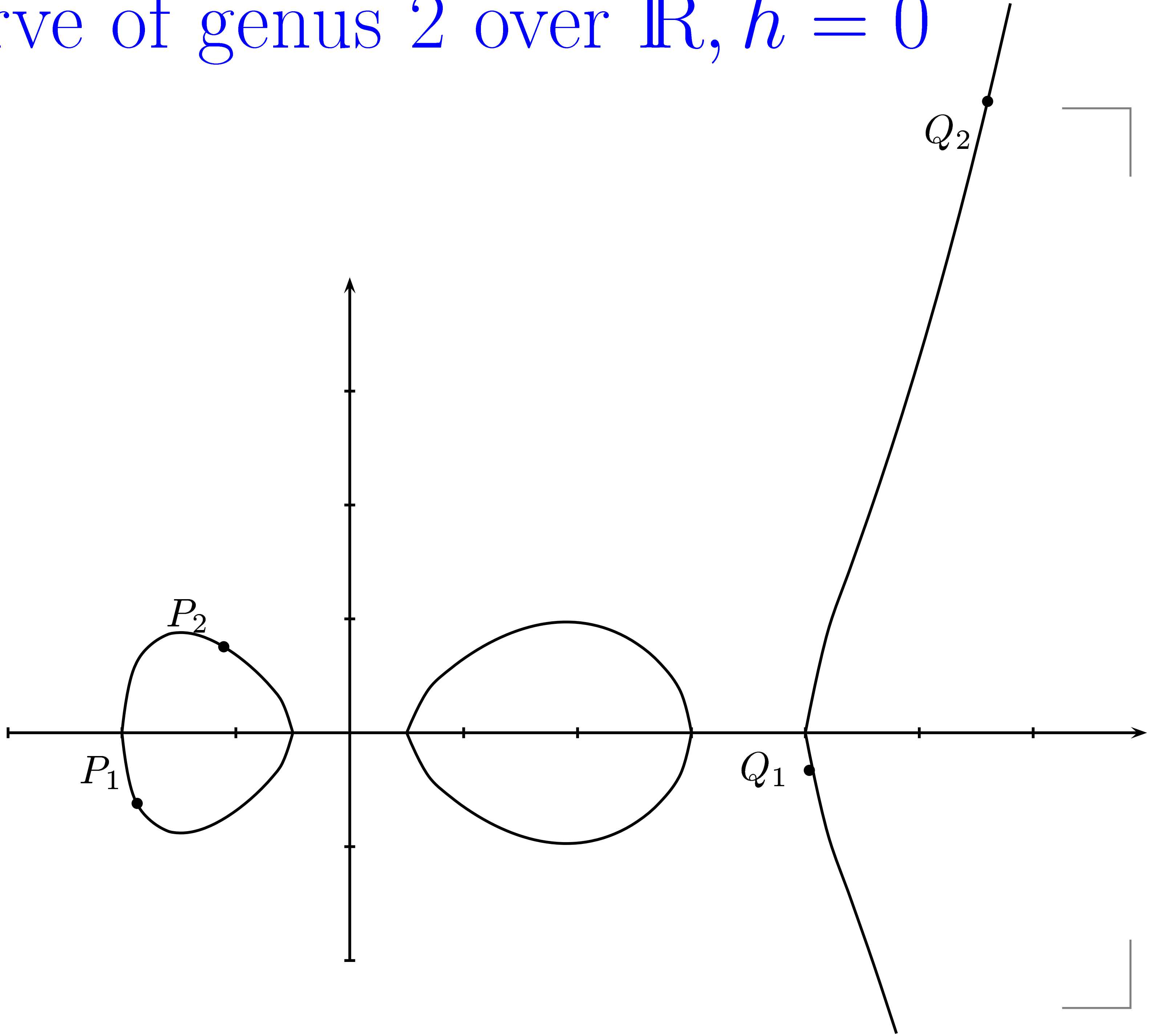
Riemann-Roch allows to find a unique reduced representation by means of a divisor of degree zero with $m \leq g$

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

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

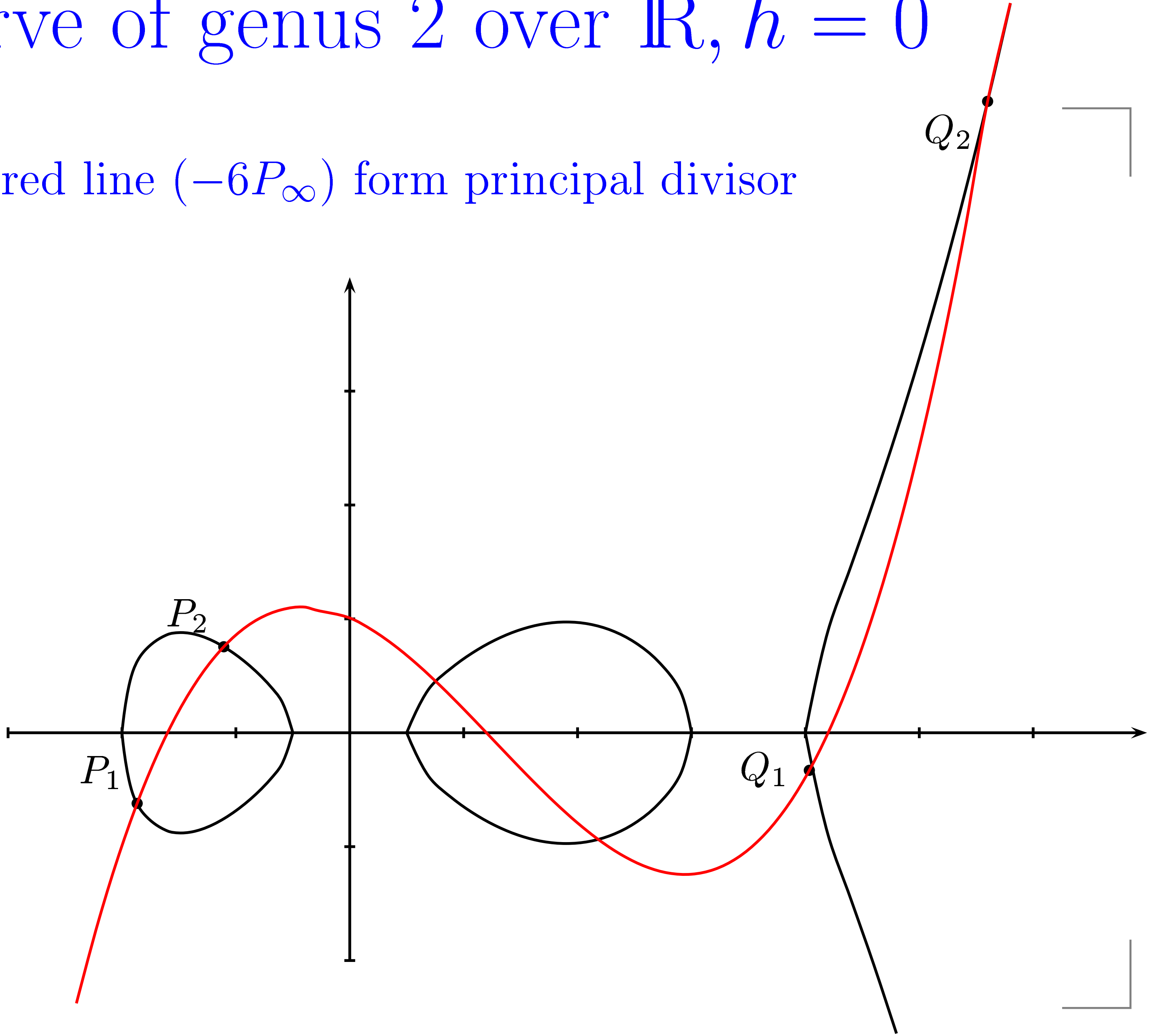
If $\bar{D}$ is defined over K, the field of definition of the P_l is bounded.

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



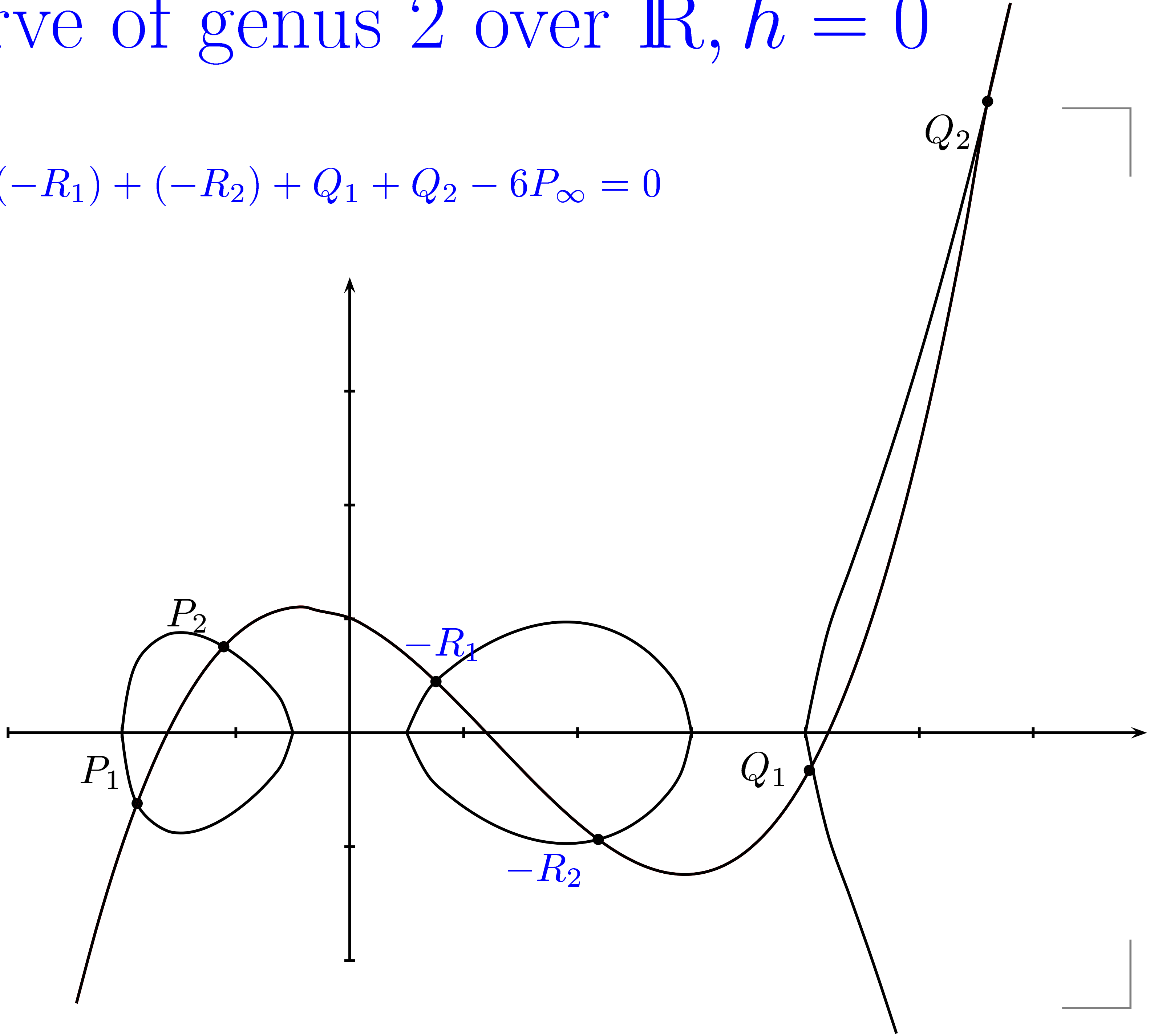
Curve of genus 2 over $\mathbb{R}$, $h = 0$

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



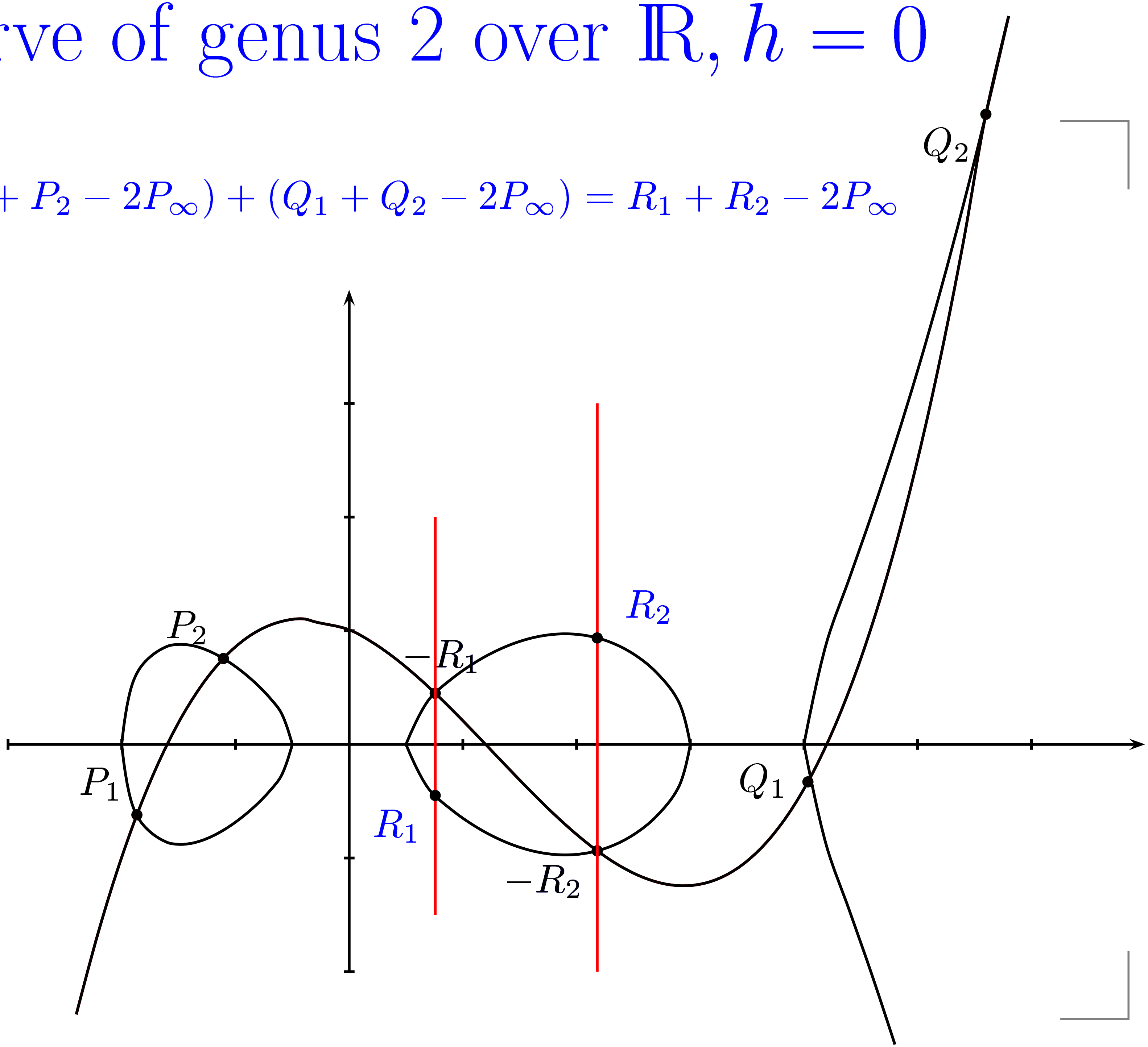
Curve of genus 2 over $\mathbb{R}$, $h = 0$

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



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

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



Mumford Representation

Divisor class group is isomorphic to
ideal class group $\mathbf{Cl}(C/\mathbb{F}_q)$ of $\mathbb{F}_q(x,y)/(C)$.
Elements D represented by two polynomials

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

u monic, $\deg v < \deg u \leq g, \quad u | v^2 + vh - f$.

$\Rightarrow$ compact representation.

Isomorphism is explicit via

$$P_i = (x_i, y_i) \Leftrightarrow u(x_i) = 0, v(x_i) = y_i \text{ with multiplicity}$$

Arithmetic uses "only" arithmetic on polynomialy ... but is far less efficient than on elliptic curves (if applied directly).

Arithmetic on hyperelliptic curves

Composition & Reduction (Cantor/Koblitz)

`IN:` $D_1 = [u_1, v_1], D_2 = [u_2, v_2], C : y^2 + h(x)y = f(x)$
`OUT:` $D = [u, v]$ reduced with $D \sim D_1 + D_2$

1. compute $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$
2. compute $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2(v_1 + v_2 + h)$
3. let $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$
4. $u = \frac{u_1 u_2}{d^2} \quad v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$
5. let $u' = \frac{f - vh - v^2}{u} \quad b' = (-h - v) \bmod u'$
6. if $\deg u' > g$ put $u := u', v := v'$ goto step 5
7. make u monic

Arithmetic in $\mathbf{Cl}(C/\mathbb{F}_q)$

2000 Harley (odd char.)
2001 L. (arbitrary char.)
2001 Matsuo, Chao, Tsujii (faster)

$\Rightarrow$ 2 inversions

2002 Miyamoto, Doi, Matsuo, Chao, Tsujii
2002 Takahashi
2002 L. (arbitrary char.)
2002 Sugizaki, Matsuo, Chao, Tsujii (even char.)

$\Rightarrow$ 1 inv.

genus 3

2002 Kuroki, Gonda, Matsuo, Chao, Tsujii
2002 Pelzl, Guyot & Patankar

$\Rightarrow$ 1 inv.

Addition, $g = 2$

Addition, $\deg u_1 = \deg u_2 = 2$		
Input	$[u_1, v_1], [u_2, v_2], u_i = x^2 + u_{i1}x + u_{i0}, v_i = v_{i1}x + v_{i0}$	
Output	$[u', v'] = [u_1, v_1] + [u_2, v_2]$	
Step	Expression	Operations
1	compute resultant r of u_1, u_2: $z_1 = u_{11} - u_{21},\ z_2 = u_{20} - u_{10},\ z_3 = u_{11}z_1 + z_2;$ $r = z_2 z_3 + z_1^2 u_{10};$	1S, 3M
2	compute almost inverse of u_2 modulo u_1 ($inv = r/u_2 \bmod u_1$): $inv_1 = z_1,\ inv_0 = z_3;$	
3	compute $s' = rs \equiv (v_1 - v_2)inv \bmod u_1$: $w_0 = v_{10} - v_{20},\ w_1 = v_{11} - v_{21},\ w_2 = inv_0 w_0,\ w_3 = inv_1 w_1;$ $s_1' = (inv_0 + inv_1)(w_0 + w_1) - w_2 - w_3(1 + u_{11}),\ s_0' = w_2 - u_{10}w_3;$ if $s_1' = 0$ see below	5M
4	compute $s'' = x + s_0/s_1 = x + s_0'/s_1'$ and s_1: $w_1 = (rs_1')^{-1}(= 1/r^2 s_1),\ w_2 = rw_1(= 1/s_1'),\ w_3 = {s'}_1^2 w_1(= s_1);$ $w_4 = rw_2(= 1/s_1),\ w_5 = w_4^2,\ s_0'' = s_0' w_2;$	I, 2S, 5M
5	compute $l' = s'' u_2 = x^3 + l_2' x^2 + l_1' x + l_0'$: $l_2' = u_{21} + s_0'',\ l_1' = u_{21}s_0'' + u_{20},\ l_0' = u_{20}s_0''$	2M
6	compute $u' = (s(l + h + 2v_2) - k)/u_1 = x^2 + u_1' x + u_0'$: $u_0' = (s_0'' - u_{11})(s_0'' - z_1 + h_2 w_4) - u_{10} + l_1' + (h_1 + 2v_{21})w_4 + (2u_{21} + z_1 - f_4)w_5;$ $u_1' = 2s_0'' - z_1 + h_2 w_4 - w_5;$	3M
7	compute $v' \equiv -h - (l + v_2) \bmod u' = v_1' x + v_0'$: $w_1 = l_2' - u_1',\ w_2 = u_1' w_1 + u_0' - l_1',\ v_1' = w_2 w_3 - v_{21} - h_1 + h_2 u_1';$ $w_2 = u_0' w_1 - l_0',\ v_0' = w_2 w_3 - v_{20} - h_0 + h_2 u_0';$	4M
total		I, 3S, 22M

Different Coordinates $g = 2$

affine $\mathcal{A}$:

$$D \sim [x^2 + u_1 x + u_0, v_1 x + v_0] \sim [u_1, u_0, v_1, v_0]$$

projective $\mathcal{P}$: Miyamoto, Doi, Matsuo, Chao, and Tsujii; L.; all 2002

$$D \sim [U_1, U_0, V_1, V_0, Z] \sim [U_1/Z, U_0/Z, V_1/Z, V_0/Z]$$

new $\mathcal{N}$: L. 2002, contains also mixed coordinates

$$D \sim [U_1, U_1, V_1, V_0, Z_1, Z_2] \sim [U_1/Z_1^2, U_0/Z_1^2, V_1/(Z_1^3 Z_2), V_0/(Z_1^3 Z_2)]$$

$\mathcal{P}$ and $\mathcal{N}$: no inversions

Comparison - odd characteristic

Doubling		Addition	
operation	costs	operation	costs
$2\mathcal{N} = \mathcal{P}$	7S, 38M	$\mathcal{N} + \mathcal{N} = \mathcal{P}$	7S, 51M
$2\mathcal{P} = \mathcal{P}$	6S, 38M	$\mathcal{N} + \mathcal{P} = \mathcal{P}$	4S, 51M
$2\mathcal{N} = \mathcal{N}$	7S, 34M	$\mathcal{N} + \mathcal{N} = \mathcal{N}$	7S, 47M
$2\mathcal{P} = \mathcal{N}$	6S, 34M	$\mathcal{N} + \mathcal{P} = \mathcal{N}$	4S, 48M
		$\mathcal{P} + \mathcal{P} = \mathcal{P}$	4S, 47M
		$\mathcal{P} + \mathcal{P} = \mathcal{N}$	4S, 44M
		$\mathcal{A} + \mathcal{N} = \mathcal{P}$	5S, 40M
		$\mathcal{A} + \mathcal{P} = \mathcal{P}$	3S, 40M
		$\mathcal{A} + \mathcal{N} = \mathcal{N}$	5S, 36M
		$\mathcal{A} + \mathcal{P} = \mathcal{N}$	3S, 37M
$2\mathcal{A} = \mathcal{A}$	1I, 5S, 22M	$\mathcal{A} + \mathcal{A} = \mathcal{A}$	1I, 3S, 22M

Implementations and Comparison

- software: for $\log_2 p \sim 40 - 60$ inversions cheap,
  use $\mathcal{A}$ for $g = 1, 2$.
  Comparison depends on I/M genus
  Paper by Roberto Avanzi (Bocum) at CHES '04, library for small p.
- hardware: usually expensive inversions,
  compute multiple of affine point via $2\mathcal{N} = \mathcal{N}, \mathcal{A} + \mathcal{N} = \mathcal{N}$,
  compute multiple of non-normalized point via
  $2\mathcal{N} = \mathcal{N}$, $\mathcal{N} + \mathcal{P} = \mathcal{N}$.
  - First implementation by Kim Nguyen (Philips) presented at ECC 2002 using $\mathcal{P}$ is half as fast as elliptic
  - Many results at RUB, ...

Field of even characteristic

Curves over $\mathbb{F}_{2^n}$

$$C : y^2 + (h_2x^2 + h_1x + h_0)y = f(x), \deg h \geq 1.$$

Above formulas hold for general equation. Get higher efficiency by specializing to type of h.
If $\deg h = 1$ the curve has 2-rank 1, which is a special property but does not weaken the system up to our present knowledge.
For odd n one can make h monic.
If $\deg h = 2$ and h has a root then one can achieve $h(x) = x^2 + h_1x$, otherwise $h(x) = x^2 + h_1x + h_0$. In the former case the group order is divisible by 4, in the latter by 2.

Some more isomorphic transformations are possible

Joint work with Marc Stevens

presented at SAC 2004.

Overview

	$h = X$	$h = h_1X$, h_1^{-1} small	$h = h_1X$	$h = X^2 + h_1X$, h_1^{-1} small
f_4 small	I, 6S, 5M	I, 5S, 7M	I, 5S, 9M	I, 6S, 10M
f_4 not small	n. a.	n. a.	n. a.	I, 6S, 12M

	$h = X^2 + h_1X$	$h = X^2 + h_1X + h_0$
f_4 small	I,5S, 15M	I, 6S, 21M
f_4 not small	I, 5S, 17M	n. a.

The END

Thanks!