Arithmetic of hyperelliptic curves over finite fields

Tanja Lange

Department of Mathematics

Technical University of Denmark

t.lange@mat.dtu.dk

07.10.2005

Overview

- Arithmetic on elliptic curves.
- Arithmetic on hyperelliptic curves.
- Special case of characteristic two.
- Montgomery arithmetic

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

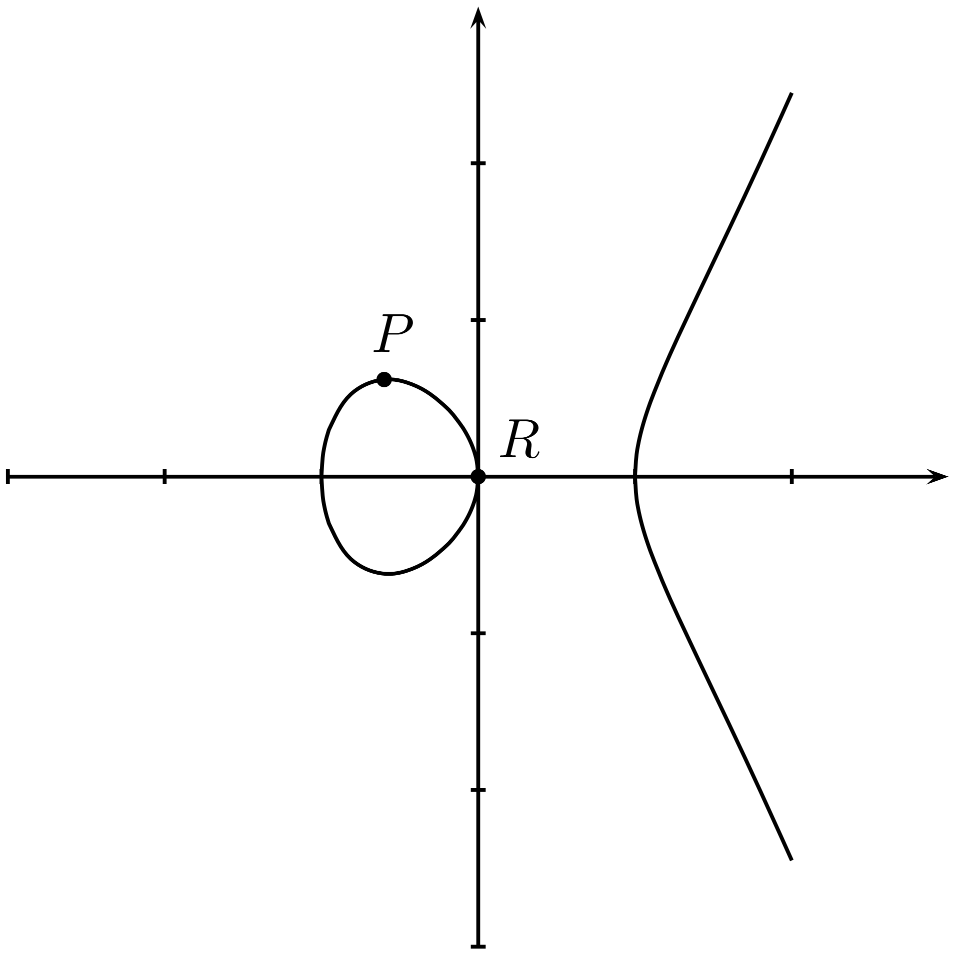
Often $q = 2^r$ or $q = p$, prime. Isomorphic transformations lead to

$$y^2 = f(x), \qquad q \text{ odd},$$

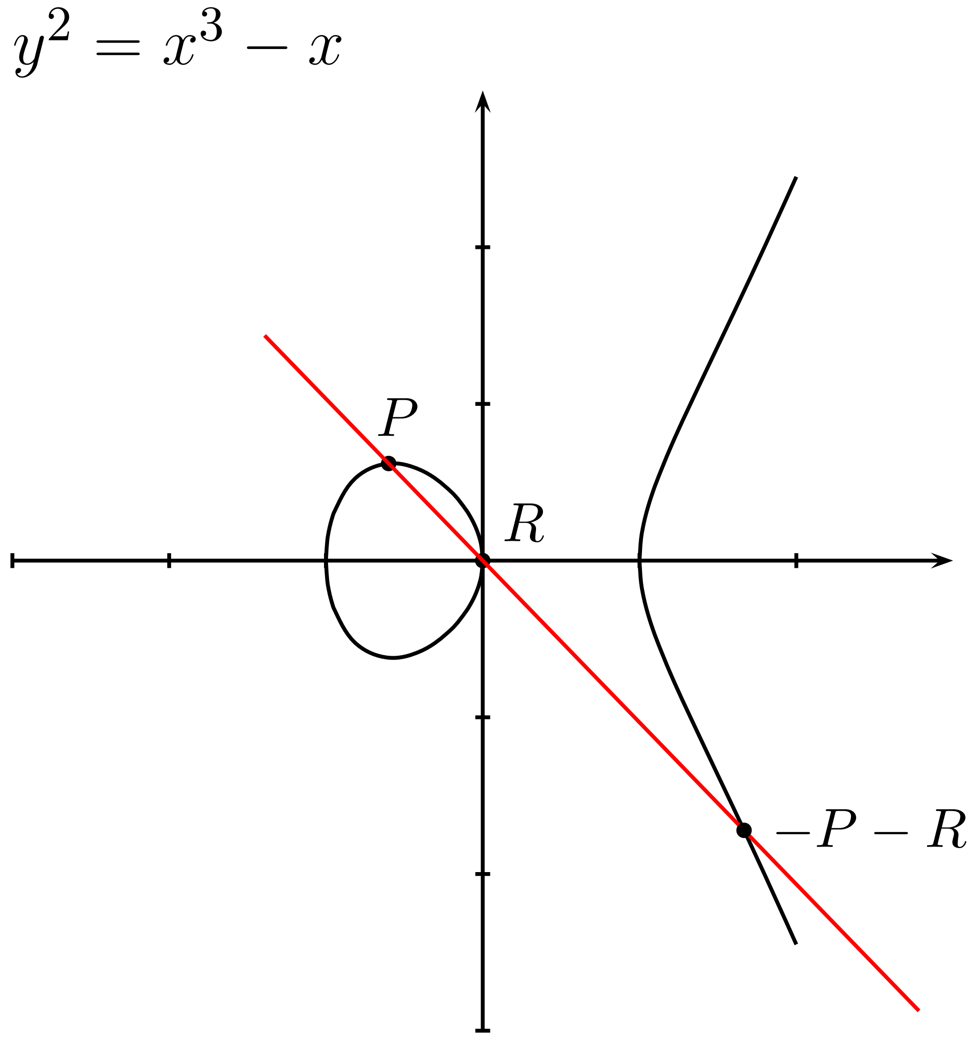
$$y^2 + xy = x^3 + ax^2 + b, \qquad q = 2^r, \text{ curve non-supersingular}$$

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

$y^2 = x^3 - x$

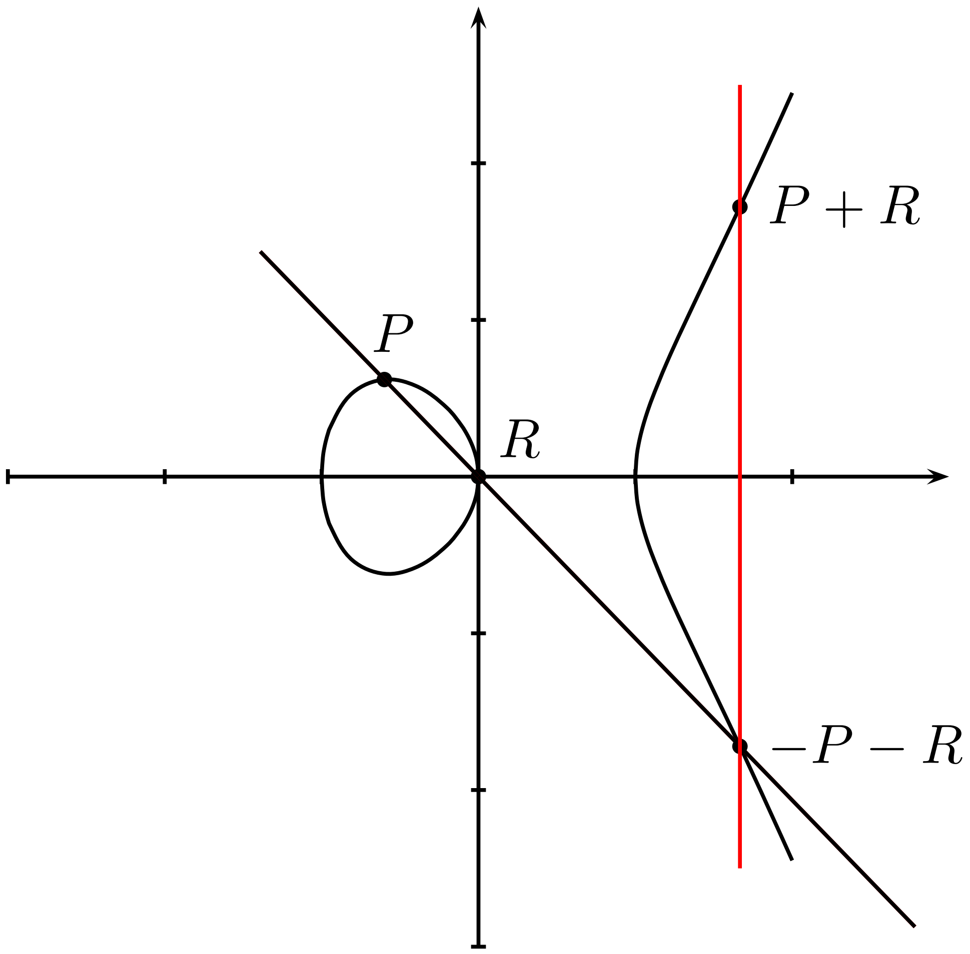


Group Law in $E(\mathbb{R}), h = 0$



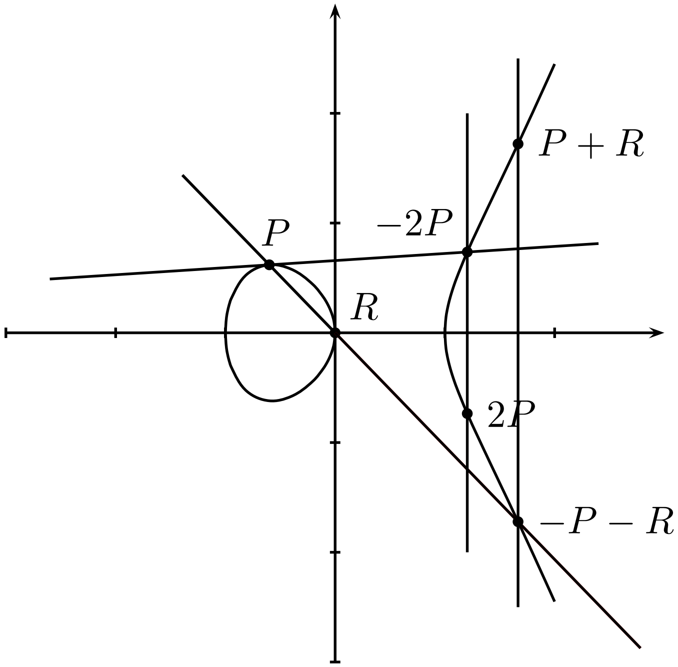
Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



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

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

Addition: 1 I, 2M, 1S
Doubling: 1 I, 2M, 2S.

Projective Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P + Q = (X_3 : Y_3 : Z_3)$
on

$$E : Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3$$

Addition: $P \neq \pm Q$

$A = Y_2 Z_1 - Y_1 Z_2, B = X_2 Z_1 - X_1 Z_2,$
$C = A^2 Z_1 Z_2 - B^3 - 2B^2 X_1 Z_2$
$X_3 = BC, Z_3 = B^3 Z_1 Z_2$
$Y_3 = A(B^2 X_1 Z_2 - C) - B^3 Y_1 Z_2,$

Doubling $P = Q \neq -P$

$A = a_4 Z_1^2 + 3X_1^2, B = Y_1 Z_1,$
$C = X_1 Y_1 B, D = A^2 - 8C$
$X_3 = 2BD, Z_3 = 8B^3.$
$Y_3 = A(4C - D) - 8Y_1^2 B^2$

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

Jacobian Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P + Q = (X_3 : Y_3 : Z_3)$
on

$$Y^2 = X^3 + a_4 X Z^4 + a_6 Z^6$$

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	–

Arithmetic on hyperelliptic curves

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.

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

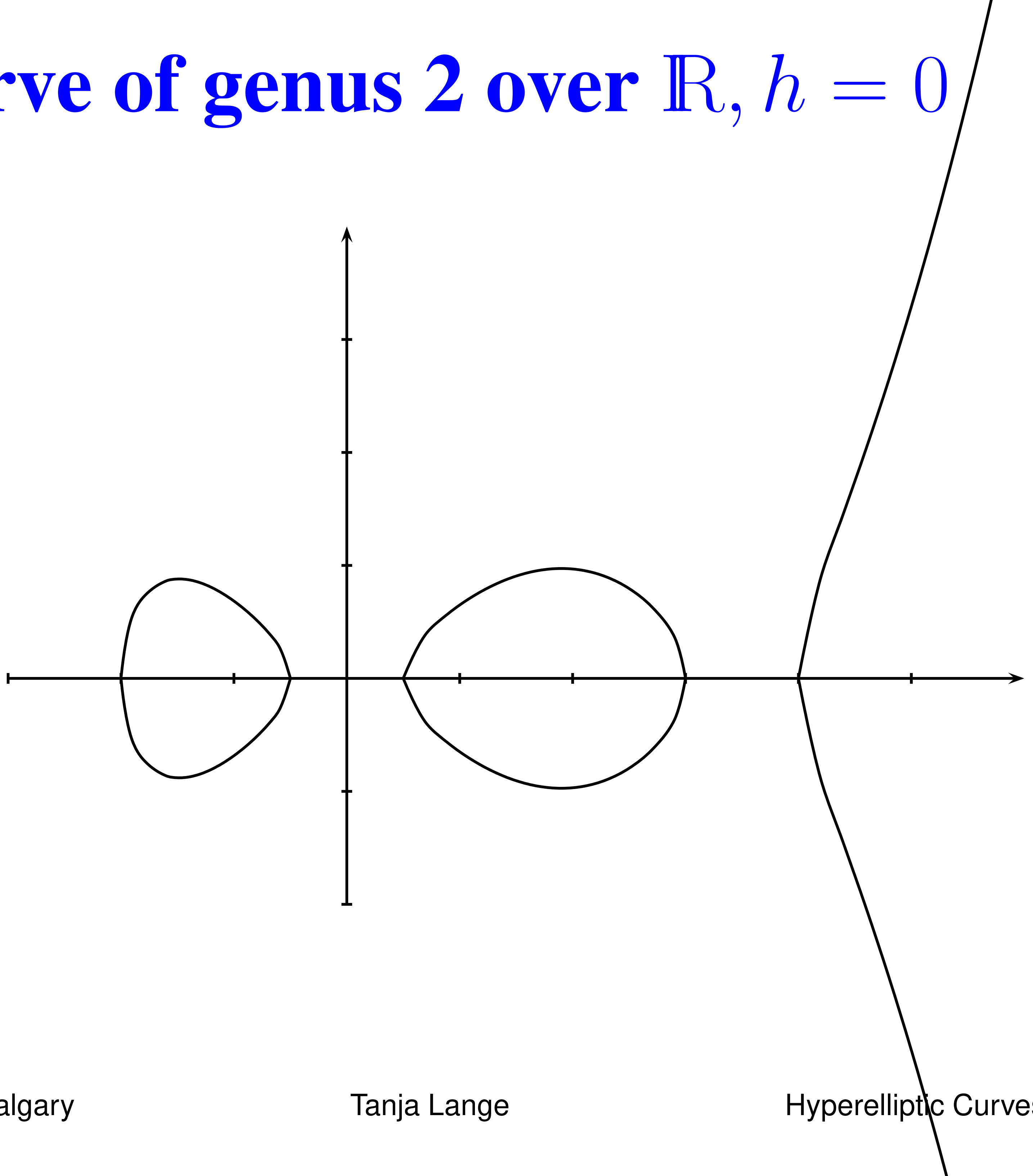
is considered as curve of genus one.

Curve of genus 2 over field of odd characteristic

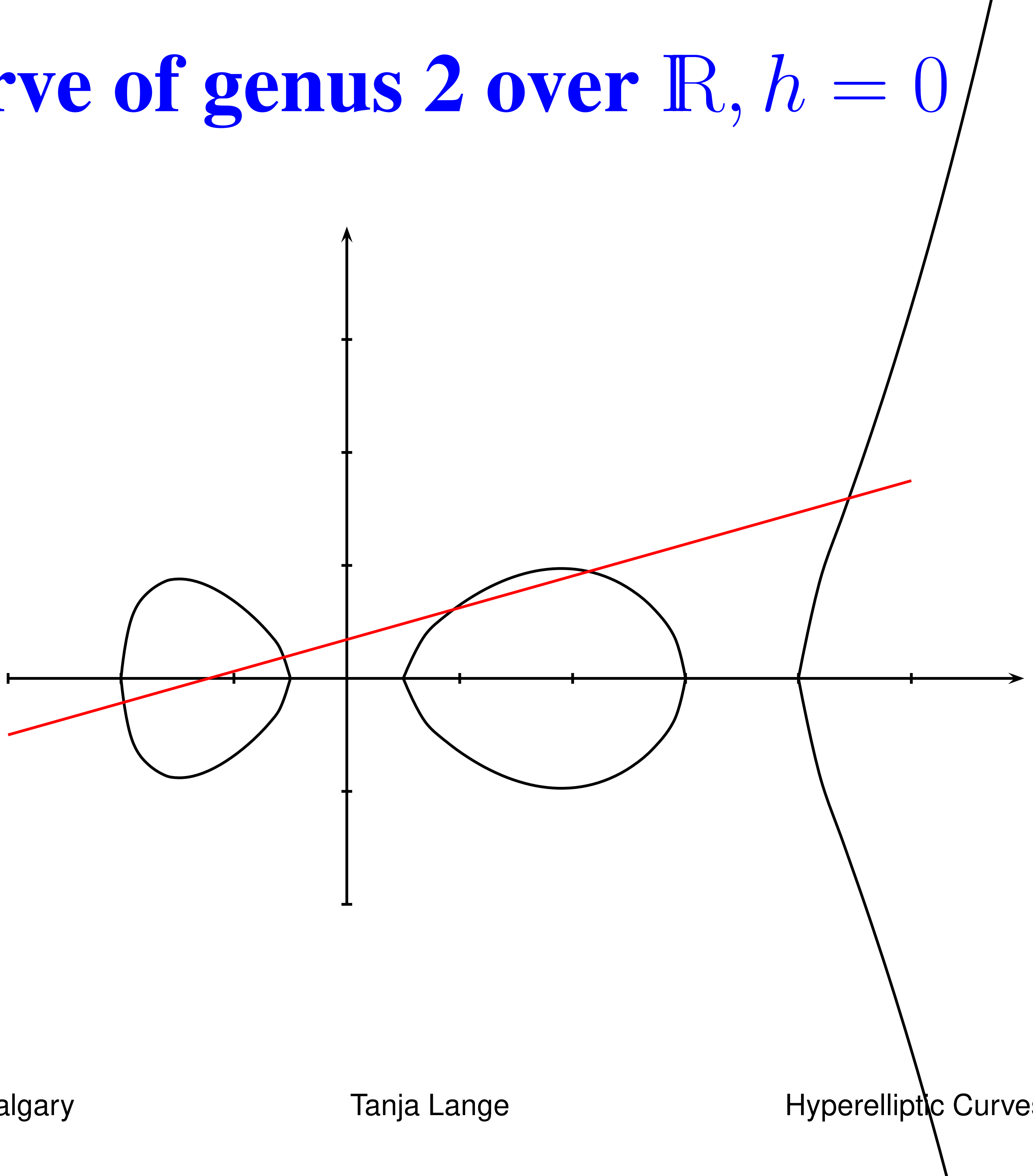
$$y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

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

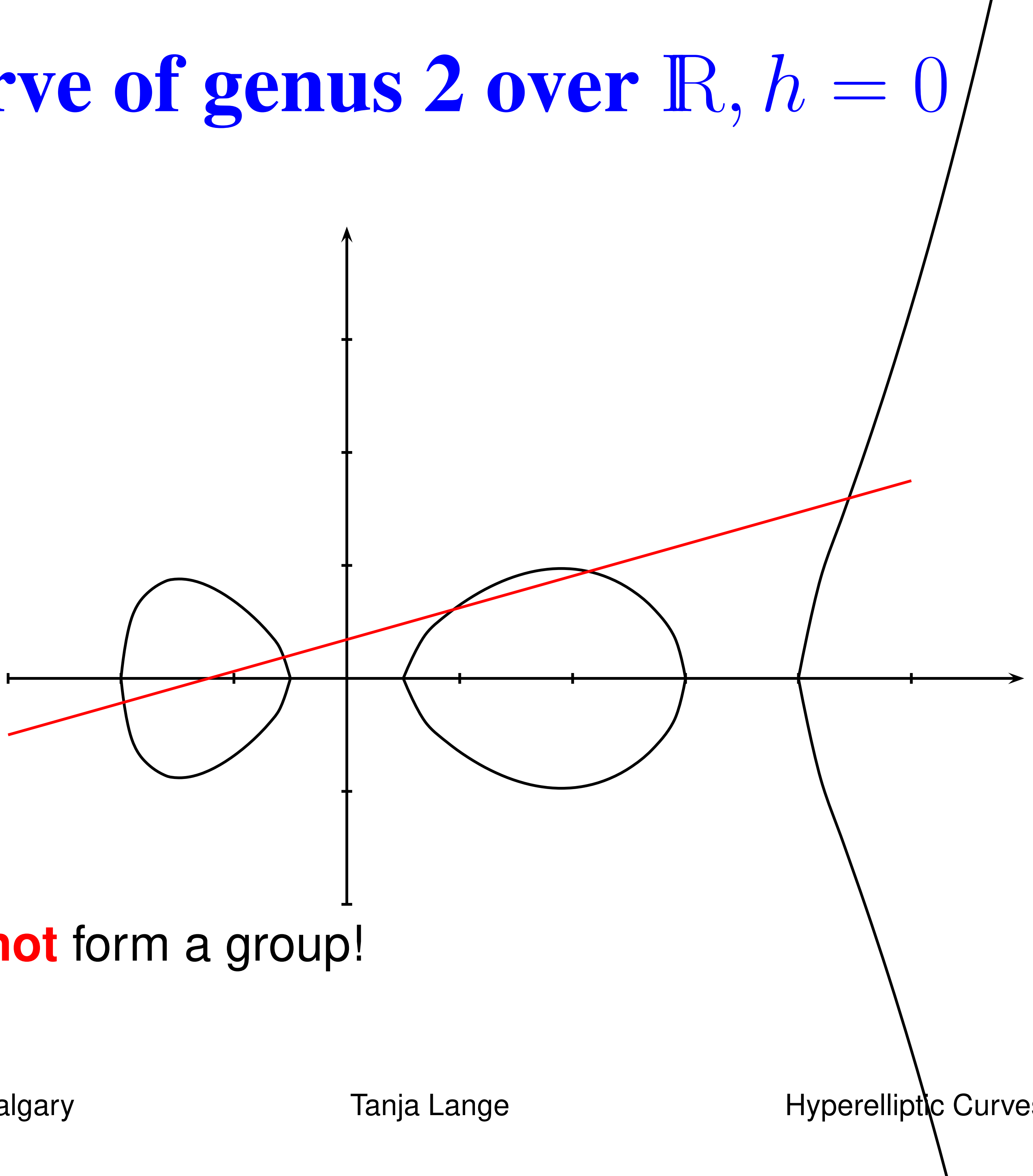
Curve of genus 2 over $\mathbb{R}$, $h = 0$



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* Princ_C.
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.

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

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

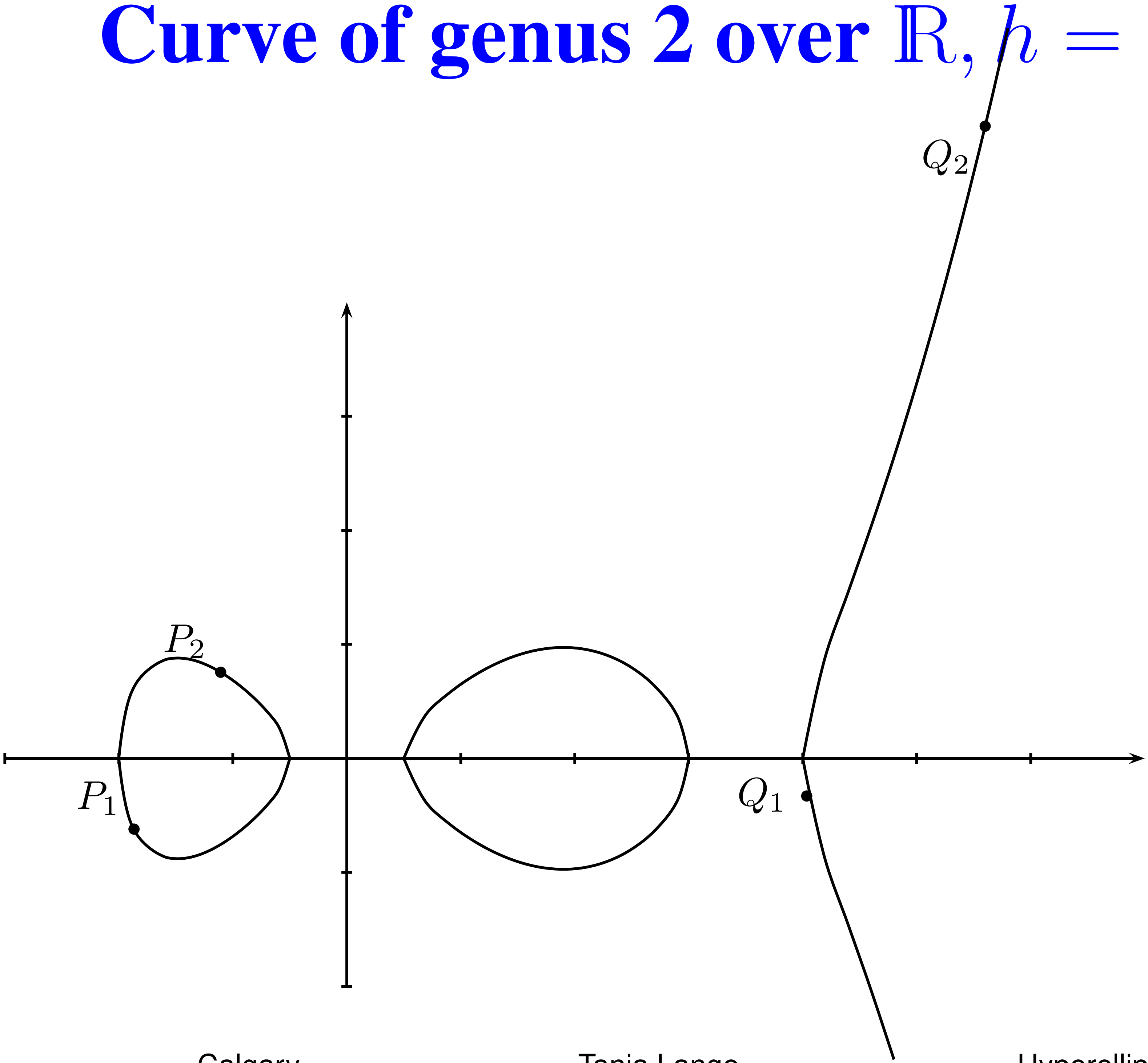
Riemann-Roch allows to find a unique reduced representation by means of a divisor of degree zero with $m \leq g$

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

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

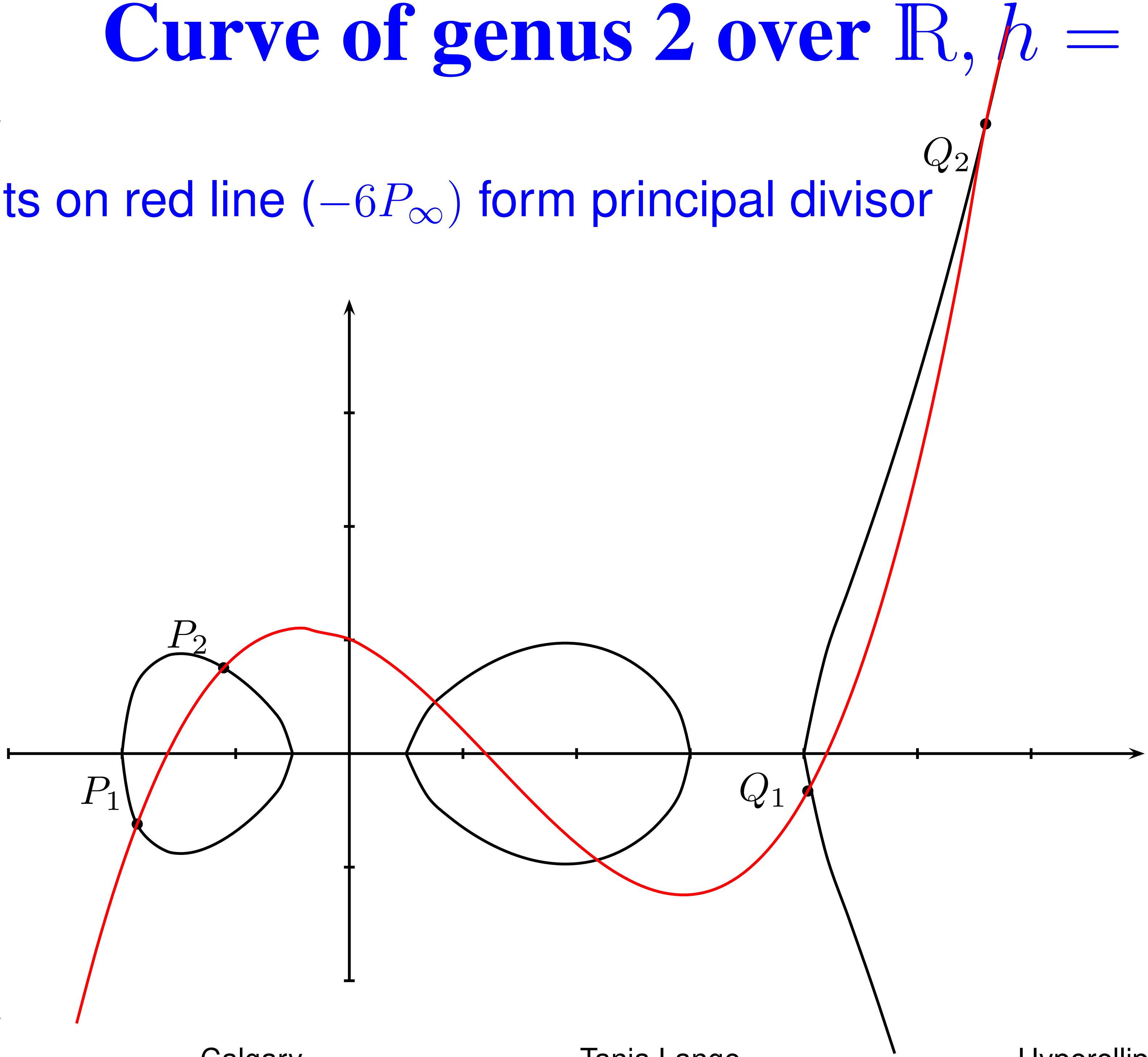
If $\bar{D}$ is defined over $\mathbb{F}_q$, the extension degree of the field of definition of the P_i is bounded, e. g. at most 2 for $g = 2$.

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



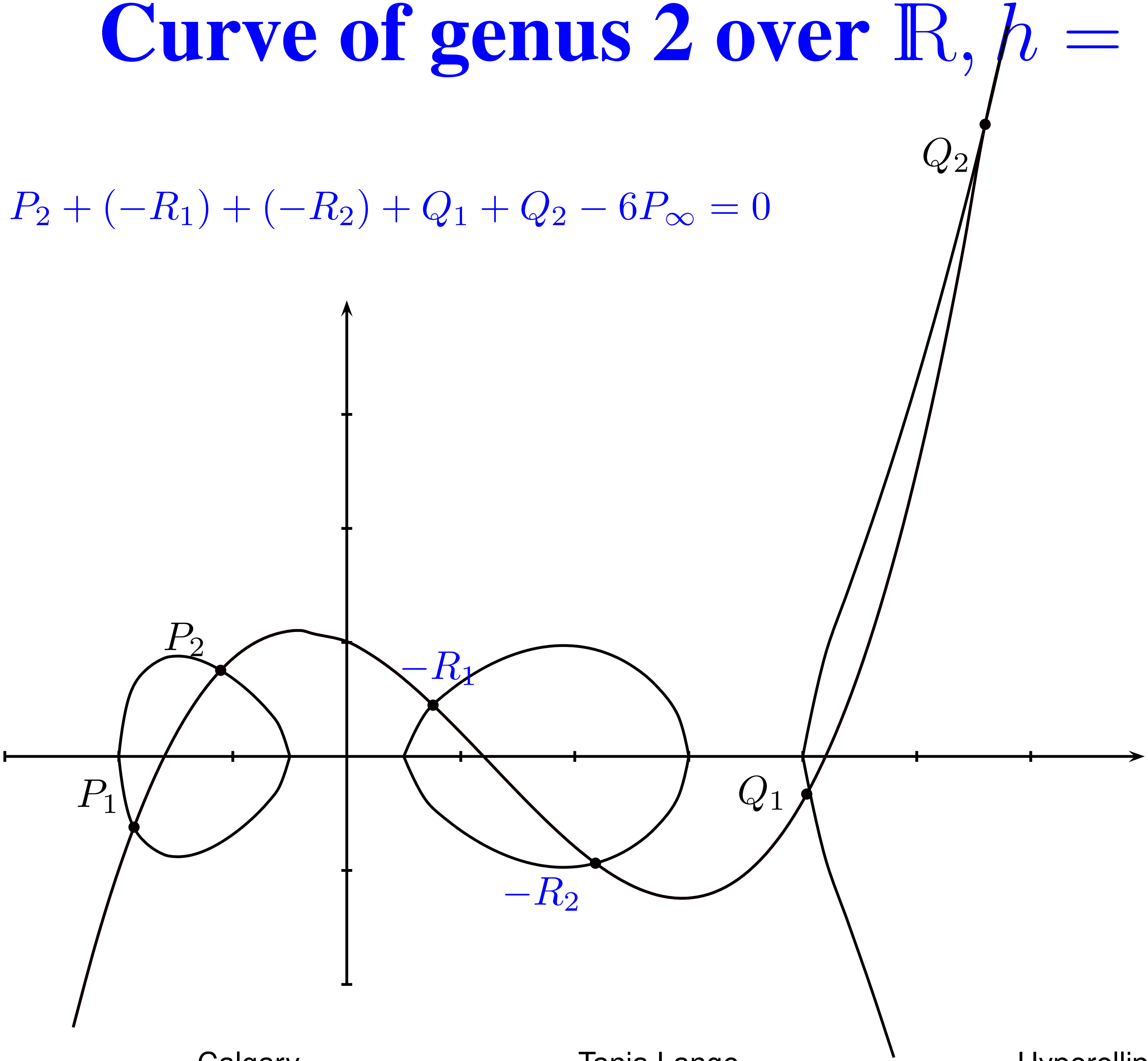
Curve of genus 2 over $\mathbb{R}$, $h = 0$

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



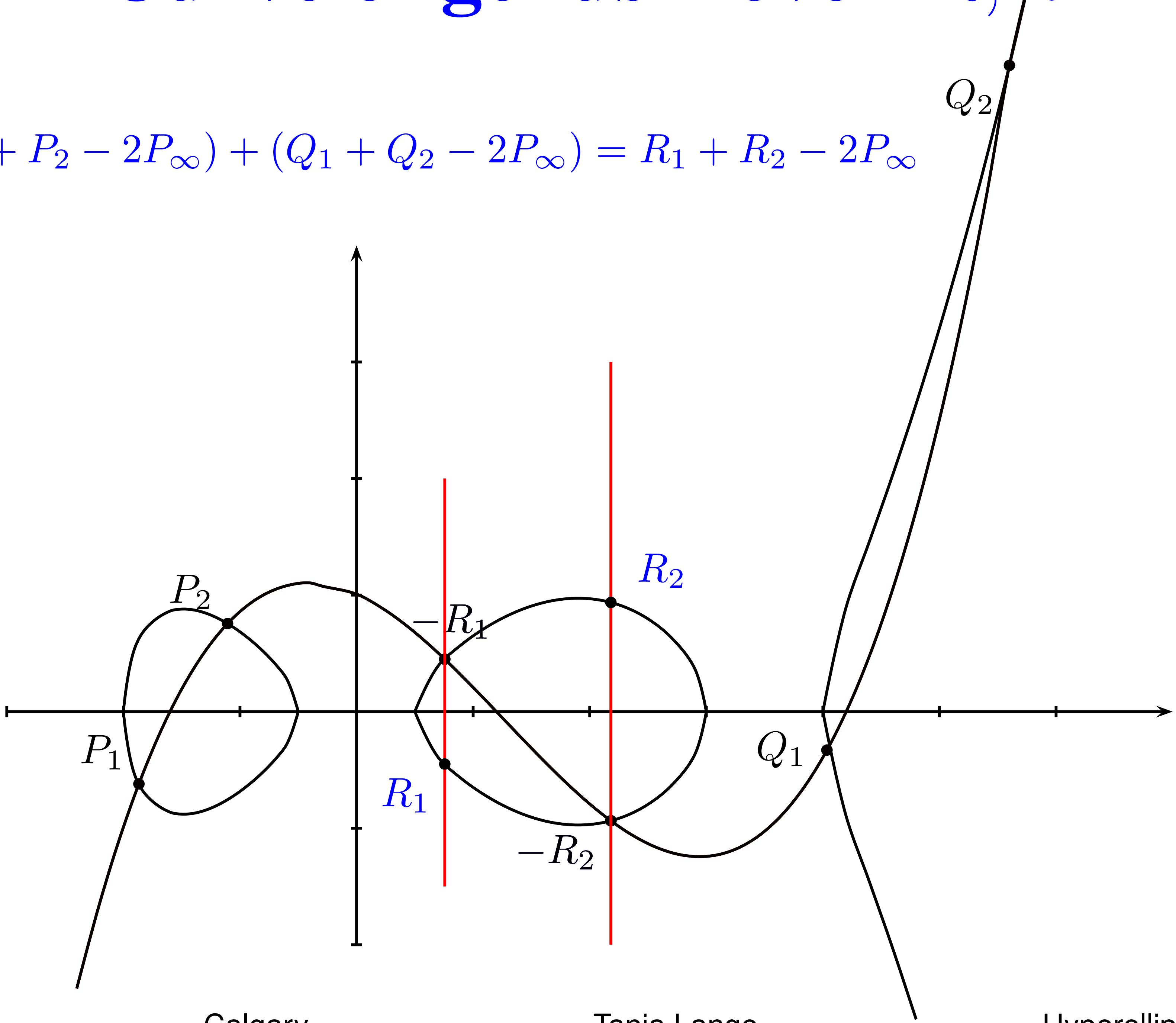
Curve of genus 2 over $\mathbb{R}$, $h = 0$

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



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

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



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

$\Rightarrow$ 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 polynomials …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

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

2000	Harley (odd char.)	$\Rightarrow$ 2 inversions
2001	L. (arbitrary char.)	
2001	Matsuo, Chao, Tsujii (faster)	
2002	Miyamoto, Doi, Matsuo, Chao, Tsujii	$\Rightarrow$ 1 inv.
2002	Takahashi	
2002	L. (arbitrary char.)	
2002	Sugizaki, Matsuo, Chao, Tsujii (even char.)	

General formulae lead to speeds comparable to ECC (Lange, Avanzi).

2004 L., Stevens $\Rightarrow$ distinction of 3 different cases, optimal affine doubling formulae for each.

General doubling, $g = 2$

Doubling, $\deg u = 2$			
Input	$[u, v], u = x^2 + u_1x + u_0, v = v_1x + v_0$		
Output	$[u', v'] = 2[u, v]$		
Step	Expression	odd	even
1	compute $\tilde{v} \equiv (h + 2v) \bmod u = \tilde{v}_1x + \tilde{v}_0$: $\tilde{v}_1 = h_1 + 2v_1 - h_2u_1, \tilde{v}_0 = h_0 + 2v_0 - h_2u_0;$		
2	compute resultant $r =$res$(\tilde{v}, u)$: $w_0 = v_1^2, w_1 = u_1^2, w_2 = \tilde{v}_1^2, w_3 = u_1\tilde{v}_1, r = u_0w_2 + \tilde{v}_0(\tilde{v}_0 - w_3);$	2S, 3M $(w_2 = 4w_0)$	2S, 3M (see below)
3	compute almost inverse $inv' = invr$: $inv'_1 = -\tilde{v}_1, inv'_0 = \tilde{v}_0 - w_3;$		
4	compute $k' = (f - hv - v^2)/u \bmod u = k'_1x + k'_0$: $w_3 = f_3 + w_1, w_4 = 2u_0, k'_1 = 2(w_1 - f_4u_1) + w_3 - w_4 - h_2v_1;$ $k'_0 = u_1(2w_4 - w_3 + f_4u_1 + h_2v_1) + f_2 - w_0 - 2f_4u_0 - h_1v_1 - h_2v_0;$	1M	2M (see below)
5	compute $s' = k'inv' \bmod u$: $w_0 = k'_0inv'_0, w_1 = k'_1inv'_1, s'_1 = (inv'_0 + inv'_1)(k'_0 + k'_1) - w_0 - w_1(1 + u_1), s'_0 = w_0 - u_0w_1;$	5M	5M
6	compute $s'' = x + s_0/s_1$ and s_1: $w_1 = 1/(rs'_1)(= 1/r^2s_1), w_2 = rw_1(= 1/s'_1), w_3 = s'^2_1w_1(= s_1);$ $w_4 = rw_2(= 1/s_1), w_5 = w_4^2, s''_0 = s'_0w_2;$	I, 2S, 5M	I, 2S, 5M
7	compute $l' = s''u = x^3 + l'_2x^2 + l'_1x + l'_0$: $l'_2 = u_1 + s''_0, l'_1 = u_1s''_0 + u_0, l'_0 = u_0s''_0;$	2M	2M
8	compute $u' = s^2 + (h + 2v)s/u + (v^2 + hv - f)/u^2$: $u'_0 = s''^2_0 + w_4(h_2(s''_0 - u_1) + 2v_1 + h_1) + w_5(2u_1 - f_4), u'_1 = 2s''_0 + h_2w_4 - w_5;$	S, 2M	S, M
9	compute $v' \equiv -h - (l + v) \bmod u' = v'_1x + v'_0$: $w_1 = l'_2 - u'_1, w_2 = u'_1w_1 + u'_0 - l'_1, v'_1 = w_2w_3 - v_1 - h_1 + h_2u'_1;$ $w_2 = u'_0w_1 - l'_0, v'_0 = w_2w_3 - v_0 - h_0 + h_2u'_0;$	4M	4M
total		each I, 5S, 22M	

Different Coordinates $g = 2$, odd q

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

Field of characteristic 2

Joint work with Marc Stevens

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.

Isomorphic transformations

Consider e. g. $\deg g = 1$:
$x \to x' + h_0/h_1,\ y \to y'$ gives

$$\begin{aligned} {y'}^2 + h_1(x' + \frac{h_0}{h_1})y' + h_0 y' &= (x' + \frac{h_0}{h_1})^5 + f_4(x' + \frac{h_0}{h_1})^4 + \cdots \\ {y'}^2 + h_1 x' y' &= {x'}^5 + \tilde{f}_4 {x'}^4 + \tilde{f}_3 {x'}^3 + \tilde{f}_2 {x'}^2 + \tilde{f}_1 x' + \tilde{f}_0. \end{aligned}$$

Changes of the form $y \to y' + a{x'}^2 + bx'$ allow $f_4 = f_1 = 0$ and some more.
If $\mathbb{F}_q = \mathbb{F}_{2^n}$ with n one can additionally achieve $h_1 = 1, f_2 \in \mathbb{F}_2$.
Usual situation:

$$C : y^2 + h_1 xy = x^5 + f_3 x^3 + f_2 x^2 + f_0.$$

Doubling, $g = 2$, $\deg h = 1$

Doubling $\deg h = 1$, $\deg u = 2$				
Input	$[u, v], u = x^2 + u_1 x + u_0, v = v_1 x + v_0; h_1^2, h_1^{-1}$			
Output	$[u', v'] = 2[u, v]$			
Step	Expression	$h_1 = 1$	h_1^{-1} small	h_1 arbitrary
1	compute rs_1: $z_0 = u_0^2$, $k_1' = u_1^2 + f_3$; $w_0 = f_0 + v_0^2 (= rs_1'/h_1^3)$;	3S	3S	3S
2	compute $1/s_1$ and s_0'': $w_1 = (1/w_0) z_0 (= h_1/s_1)$; $z_1 = k_1' w_1$, $s_0'' = z_1 + u_1$;	I, 2M	I, 2M	I, 2M
3	compute u': $w_2 = h_1^2 w_1$, $u_1' = w_2 w_1$; $u_0' = s_0''^2 + w_2$;	2S	S, 2M	S, 2M
4	compute v': $w_3 = w_2 + k_1'$; $v_1' = h_1^{-1}(w_3 z_1 + w_2 u_1' + f_2 + v_1^2)$; $v_0' = h_1^{-1}(w_3 u_0' + f_1 + z_0)$;	S, 3M	S, 3M	S, 5M
total		I, 6S, 5M	I, 5S, 7M	I, 5S, 9M

Results

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

	$h = X^2 + h_1X$	$h = X^2 + h_1X + h_0$	all
f_4 small	I,5S, 15M	I, 6S, 21M	I, 5S, 22M
f_4 not small	I, 5S, 17M	n. a.	n. a.

Inversion Free Coordinates – $h = x$

$\mathcal{P}$: projective $u_i = U_i/Z, v_i = V_i/Z$,

$\mathcal{N}$: new $u_i = U_i/Z_1^2, v_i = V_i/Z_1^3 Z_2$

$\mathcal{R}$: recent $u_i = U_i/Z, v_i = V_i/Z^2$

Doubling		Addition	
Operation	Costs	Operation	Costs
$2\mathcal{N} = \mathcal{N}$	$28\mathrm{M} + 5\mathrm{S}$	$\mathcal{R} + \mathcal{R} = \mathcal{R}$	$49\mathrm{M} + 8\mathrm{S}$
$2\mathcal{P} = \mathcal{P}$	$22\mathrm{M} + 6\mathrm{S}$	$\mathcal{P} + \mathcal{P} = \mathcal{P}$	$49\mathrm{M} + 4\mathrm{S}$
$2\mathcal{R} = \mathcal{R}$	$20\mathrm{M} + 8\mathrm{S}$	$\mathcal{N} + \mathcal{N} = \mathcal{N}$	$42\mathrm{M} + 6\mathrm{S}$
—	—	$\mathcal{A} + \mathcal{R} = \mathcal{R}$	$42\mathrm{M} + 7\mathrm{S}$
—	—	$\mathcal{A} + \mathcal{P} = \mathcal{P}$	$39\mathrm{M} + 4\mathrm{S}$
—	—	$\mathcal{A} + \mathcal{N} = \mathcal{N}$	$36\mathrm{M} + 6\mathrm{S}$
$2\mathcal{A} = \mathcal{A}$	$\mathrm{I} + 5\mathrm{M} + 6\mathrm{S}$	$\mathcal{A} + \mathcal{A} = \mathcal{A}$	$\mathrm{I} + 21\mathrm{M} + 3\mathrm{S}$

Before best result: $2\mathcal{N} = \mathcal{N}$, 6S, 35M for $\deg h = 1$.

Montgomery Arithmetic

Montgomery Ladder (Arbitrary Group)

Idea: Make used addition per round to avoid SSCA.
Consider the intermediate results (i is decreasing).
$Q_i = \sum_{j=i}^{l} n_j 2^{j-i} P$, put $R_i = Q_i + P$, then

$$Q_i = 2Q_{i+1} + n_i P = Q_{i+1} + R_{i+1} + n_i P - P = 2R_{i+1} + n_i P - 2P.$$

This implies

$$(Q_i, R_i) = \begin{cases} (2Q_{i+1}, Q_{i+1} + R_{i+1}) & \text{if } n_i = 0 \\ (Q_{i+1} + R_{i+1}, 2R_{i+1}) & \text{if } n_i = 1 \end{cases}$$

$$13 = (1101)_2 \sim \begin{array}{rcl} (Q_3, R_3) & = & (P, 2P) \\ (Q_2, R_2) & = & (3P, 4P) \\ (Q_1, R_1) & = & (6P, 7P) \\ (Q_0, R_0) & = & (13P, 14P) \end{array}$$

Montgomery Arithmetic for EC

Advantages:

- Needs only x coordinate (not y)
  $\Rightarrow$ lower storage requirement compared to full Montgomery ladder.
- Projective version (no inversion) extremely efficient for special curves (uses x and z) $\Rightarrow$ Montgomery curves (curves were proposed for ECM factoring due to fast group operation).
- Shielded against SPA (Brier/Joye for arbitrary curves), slower than for general curves but faster than full doubling and addition and less storage needed.

Montgomery Arithmetic for Genus 2 Curves

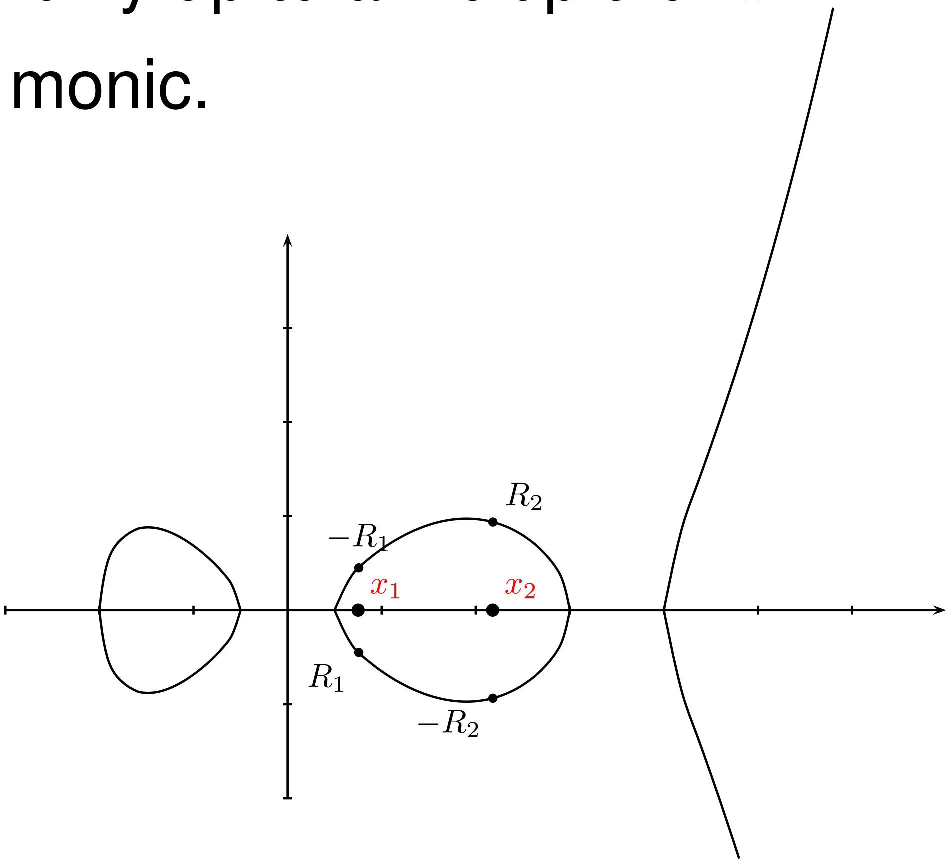
Problems:

- Reduction in $\tilde{v_\pm} = s_1u_1v_2 + s_2u_2v_1 + s_3(v_1v_2 + f) \bmod u_\pm$
- As $f \equiv v^2 \bmod u$, v^2 is given only up to a multiple of u.
- The resulting u'_+ will not be monic.

Reason:

Each u-polynomial belongs to 4 different divisor classes:

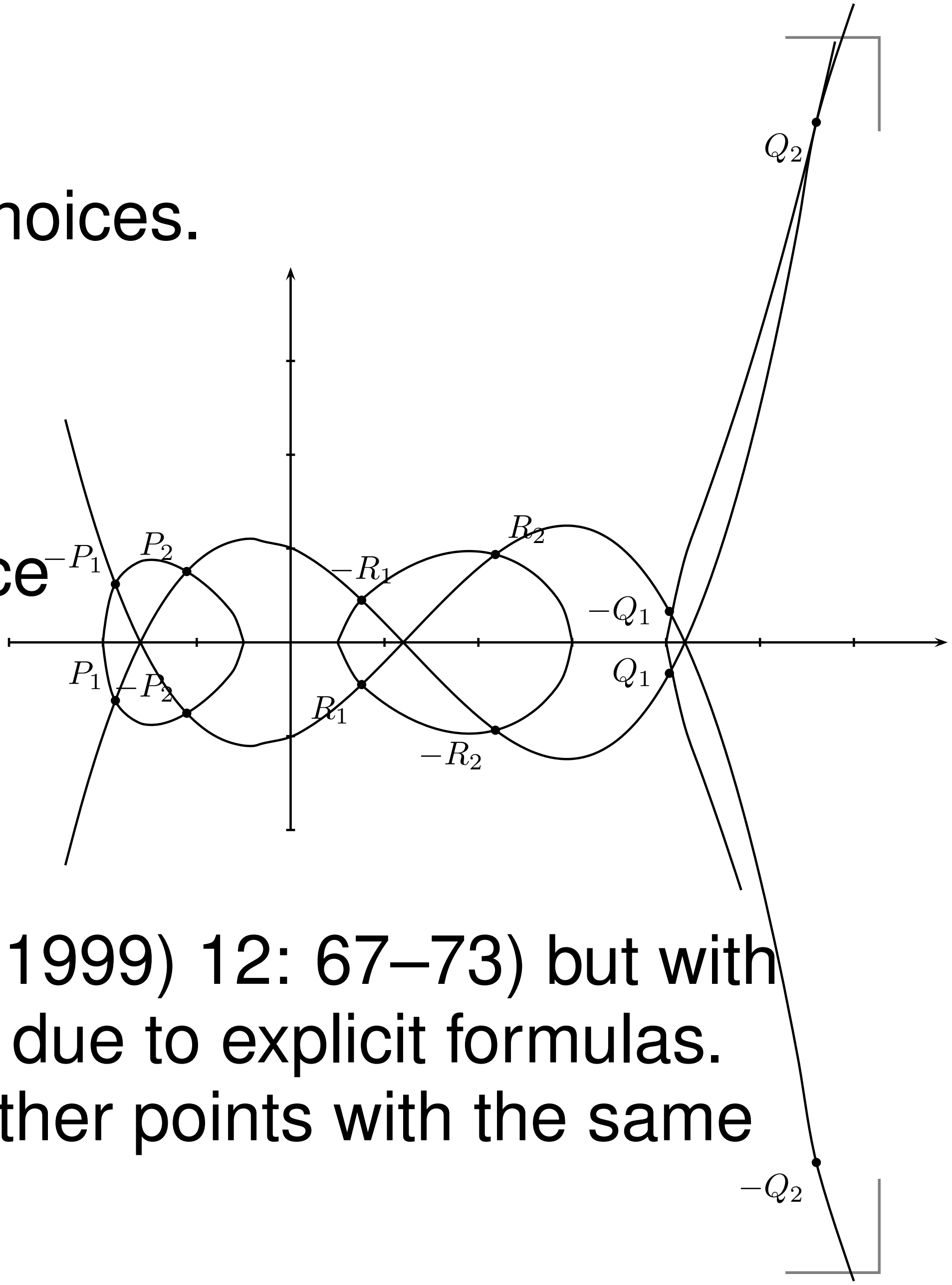
$$\begin{aligned} P_1 + R_2 &- 2P_\infty \\ (-R_1) + R_2 &- 2P_\infty \\ R_1 + (-R_2) &- 2P_\infty \\ (-R_1) + (-R_2) &- 2P_\infty \end{aligned}$$



Genus Two cont.

Additionally known: u_-
$\Rightarrow$ cancels out all but 2 possible choices.

ANTS 2005:
L.: Montgomery arithmetic for general genus 2 curves.
Duquesne: Use of Kummer surface – this requires curves with at least one 2-torsion point;



proposal similar to paper by
Smart and Siksek (J. Cryptology (1999) 12: 67–73) but with much lower number of operations due to explicit formulas.
The Kummer surface groups together points with the same x-coordinate (cf. Cassels/Flynn).

Montgomery a la Pierrick Gaudry

ePrint Report 2005/314
Fast genus 2 arithmetic based on Theta functions

- builds on Chudnovsky/Chudnovsky
- uses theta functions to map on Kummer surface, hence different description from Duquesne
- 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)
- is faster than elliptic curves in Montgomery form

The End

The END

Thanks!