

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

Tanja Lange

ITSC - Information-Security and Cryptography

Ruhr-University of Bochum

lange@itsc.ruhr-uni-bochum.de

12.08.2003

Overview

- Groups for DL-systems
- Arithmetic on elliptic curves
- Arithmetic on hyperelliptic curves
- Speed-up via endomorphisms
 - Koblitz curves
 - Generalized GLV
 - Trace zero subvariety

Diffie-Hellman Protocol

Alice

1. secretly generates

$$a < |\langle g \rangle|$$

2. computes $h_1 = a \cdot g$

3. transmits h_1

4. computes

$$a \cdot h_2$$

Bob

1. secretly generates

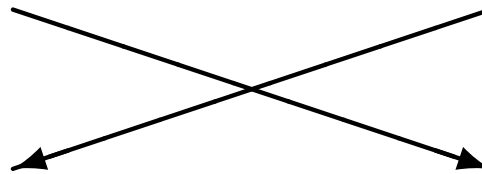
$$b < |\langle g \rangle|$$

2. computes $h_2 = b \cdot g$

3. transmits h_2

4. computes

$$b \cdot h_1$$



$$= (ab)g =$$

Common Key: the group element $k = (ab)g \in G$

Group G suitable

- group order can be computed efficiently, (avoid Pohlig-Hellman, ...)
- discrete logarithm problem is computationally hard,
- representation is easy and compact,
- scalar multiplication is fast,
⇒ key-exchange is fast.

Examples (group)

- Diffie, Hellman (1976): $G = \mathbb{F}_p^*$, i.e.

$$G = \{1, 2, \dots, p-1\}$$

- $G = \mathbb{F}_q^*$, $q = p^l$

- Koblitz/Miller (1985): $G = E(\mathbb{F}_q)$, group of points on an elliptic curve
i.e.

$$G = \{ (x, y) \in \mathbb{F}_q^2 : y^2 = x^3 + ax + b \} \cup \{ \infty \}$$

- Koblitz (1989): $G = \text{Cl}(C/\mathbb{F}_q)$, ideal class group of a hyperelliptic curve C over \mathbb{F}_q

Arithmetic on elliptic curves

Elliptic curve

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

often $q = 2^r$ or $q = p$, prime.

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

Addition law (q odd, $a_1 = a_2 = a_3 = 0$)

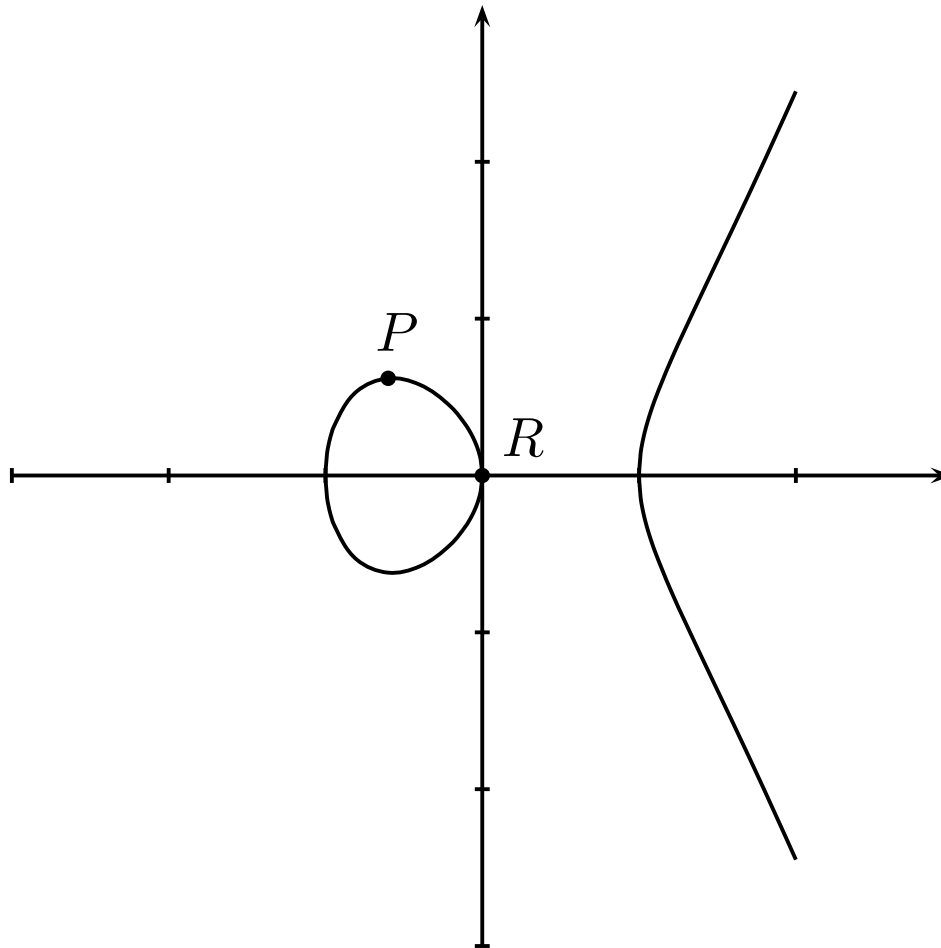
$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),$$

where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $x_1 \neq x_2$,

$$\lambda = (3x_1^2 + a_4)/(2y_1) \quad \text{else.}$$

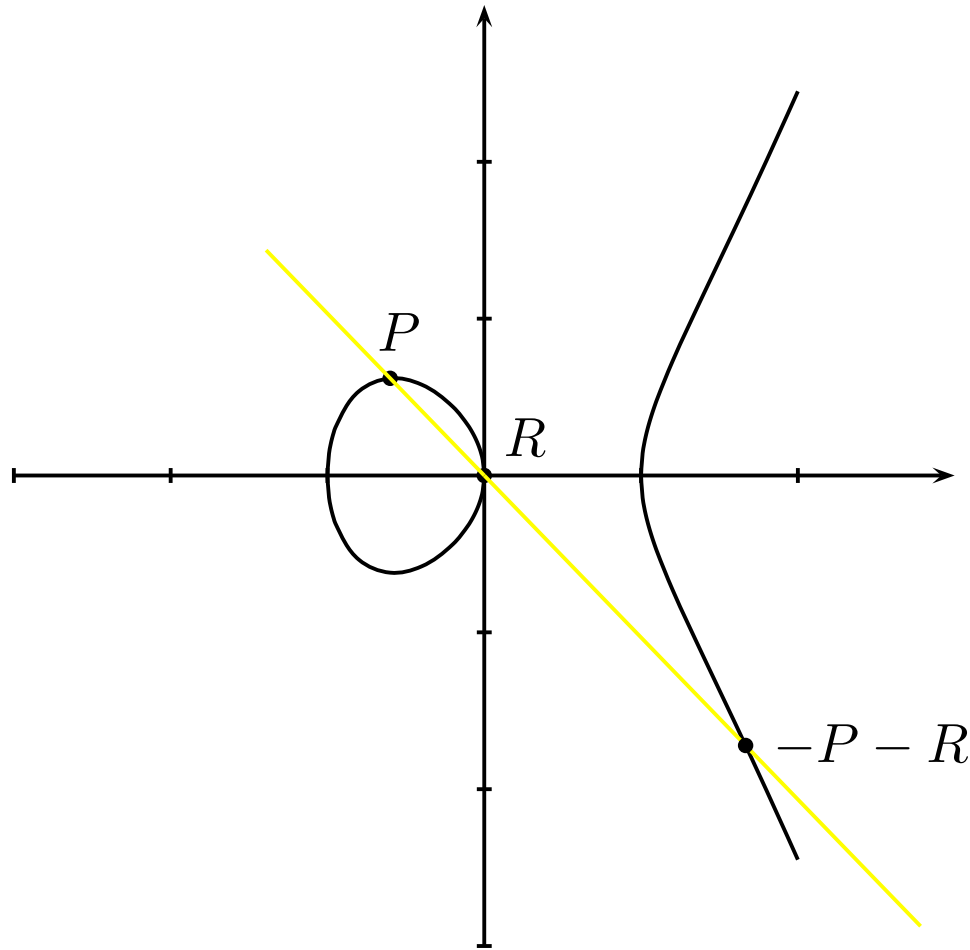
Group Law in $E(\mathbb{R})$

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



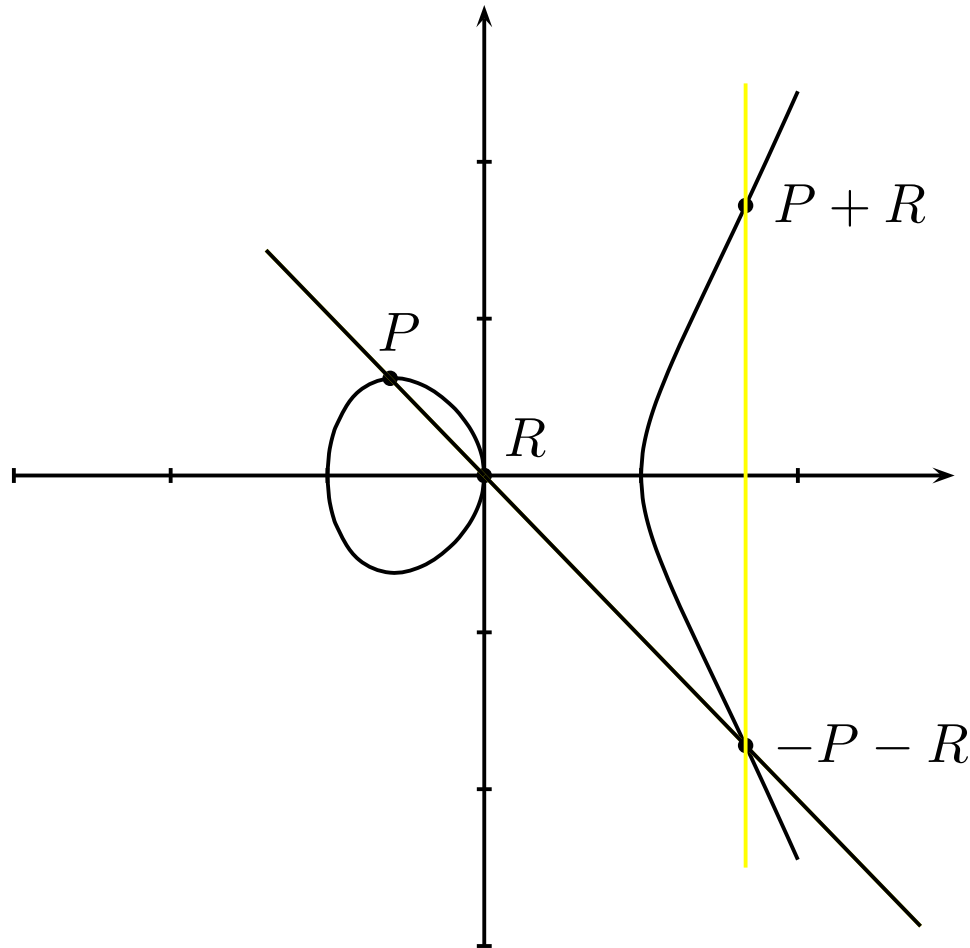
Group Law in $E(\mathbb{R})$

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



Group Law in $E(\mathbb{R})$

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



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

Hyperelliptic curve

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

$h(x), f(x) \in \mathbb{F}_q[x]$, q prime power,

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

nonsingular, i. e. not both partial derivatives zero for

$(a, b) \in C/\bar{\mathbb{F}}_q$

C **hyperelliptic curve of genus g**

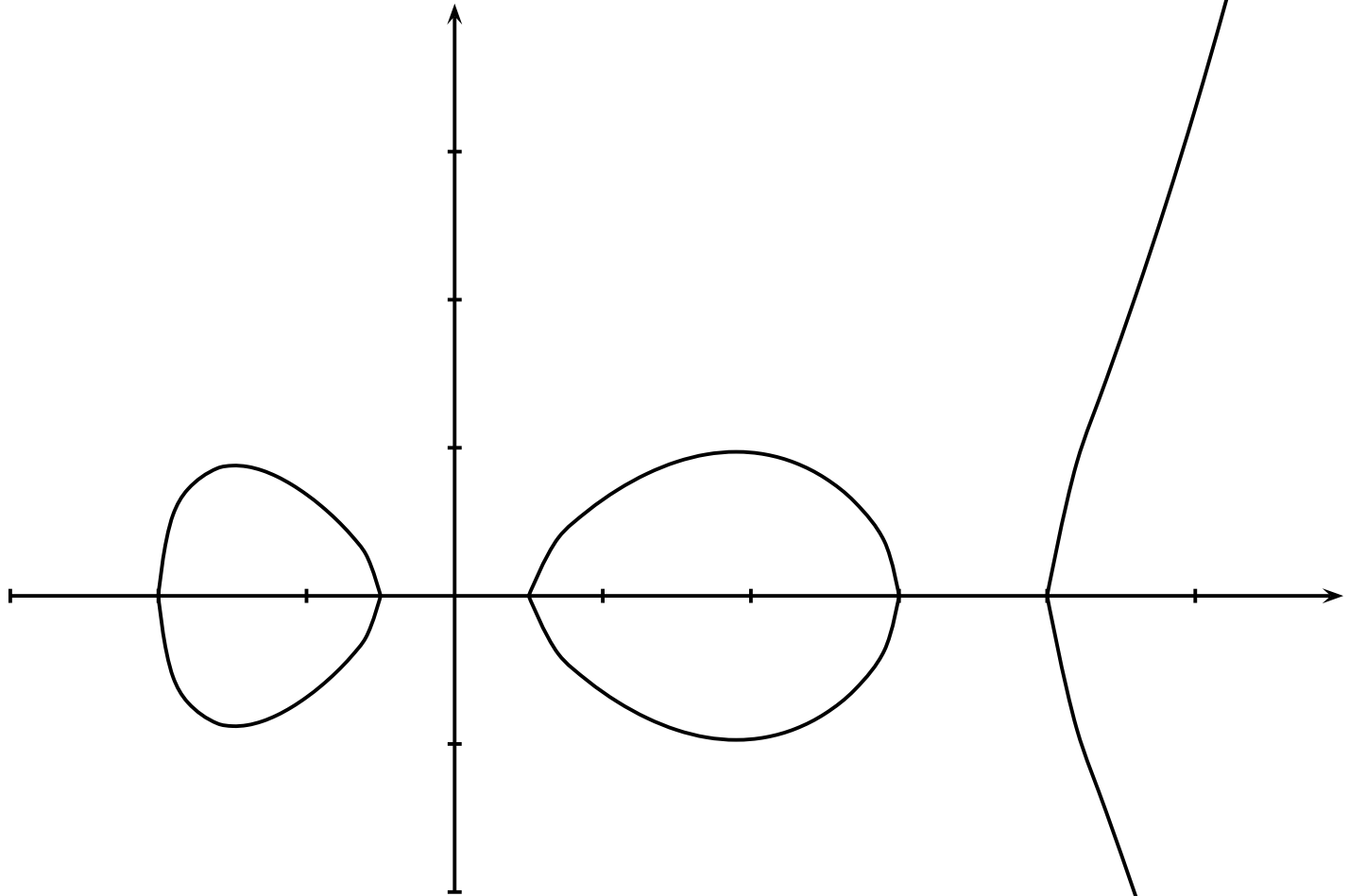
with at least one \mathbb{F}_q -rational Weierstraß point
(elliptic curves are curves of genus 1)

Example:

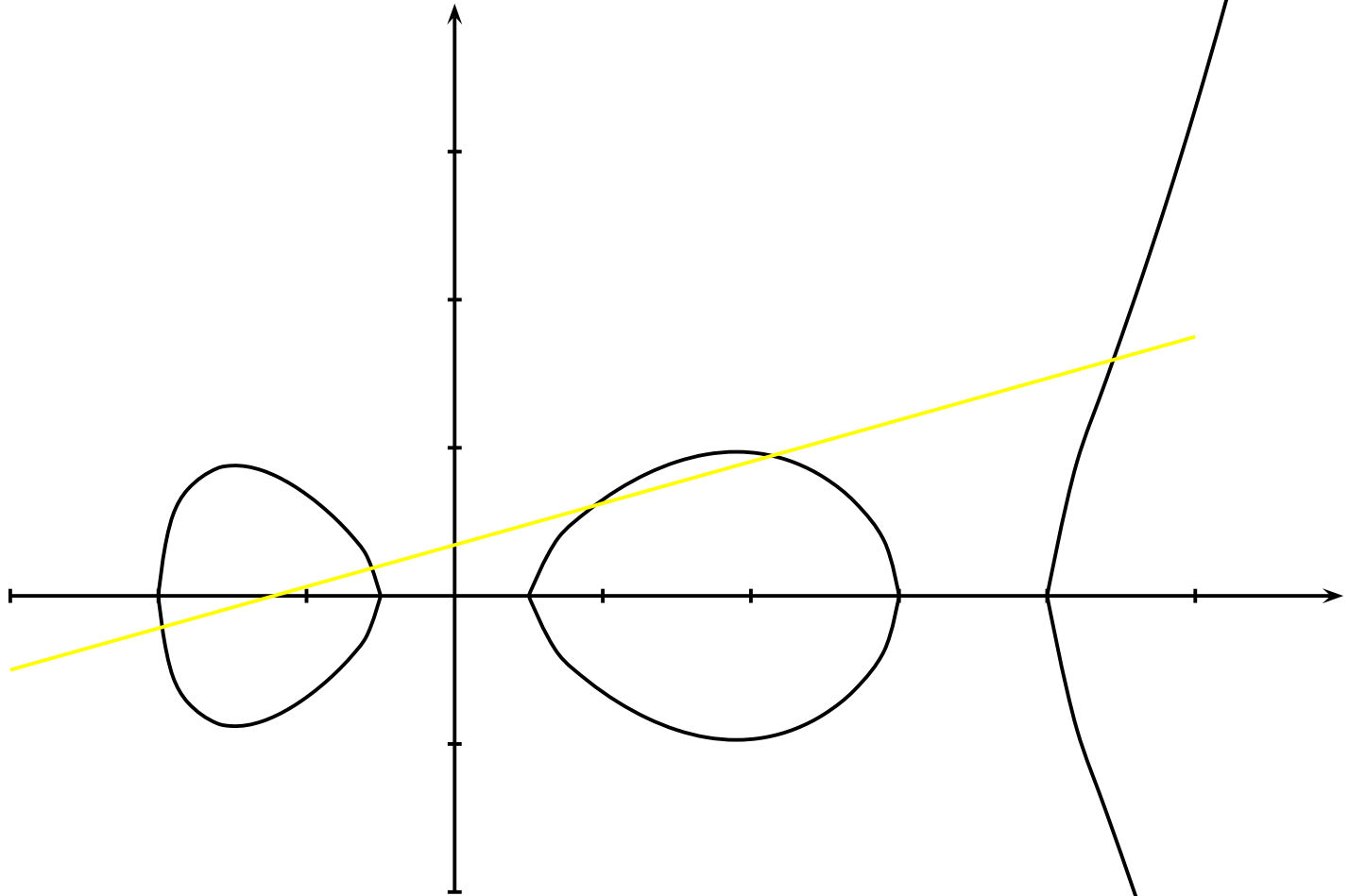
$$y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0$$

genus 2 curve over field of odd characteristic.

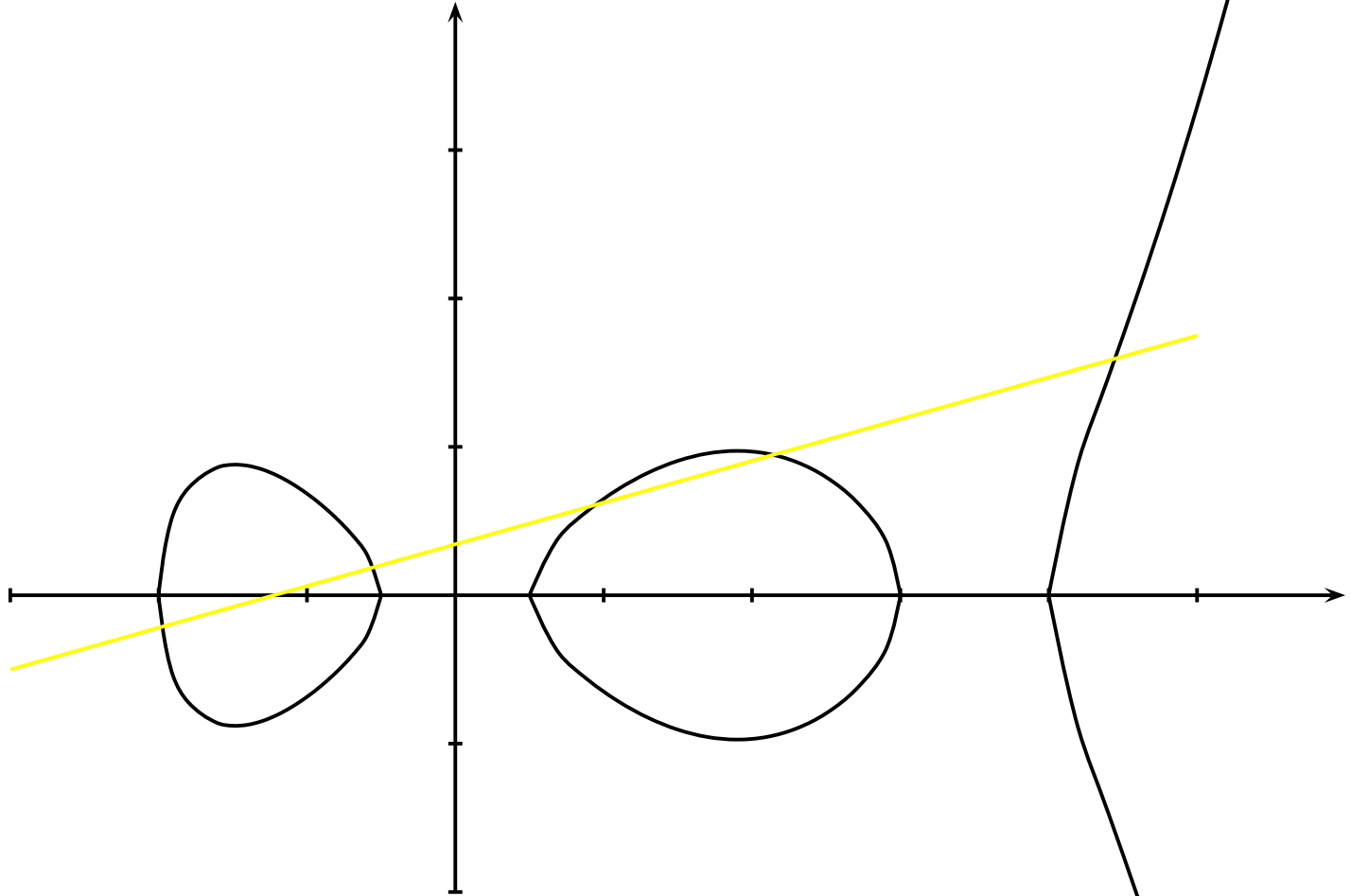
Curve of Genus 2 over \mathbb{R}



Curve of Genus 2 over \mathbb{R}



Curve of Genus 2 over \mathbb{R}



Points do **not** form a group

Group

Use **divisors**, i. e. sums of points, of degree zero and reduce modulo principal divisors

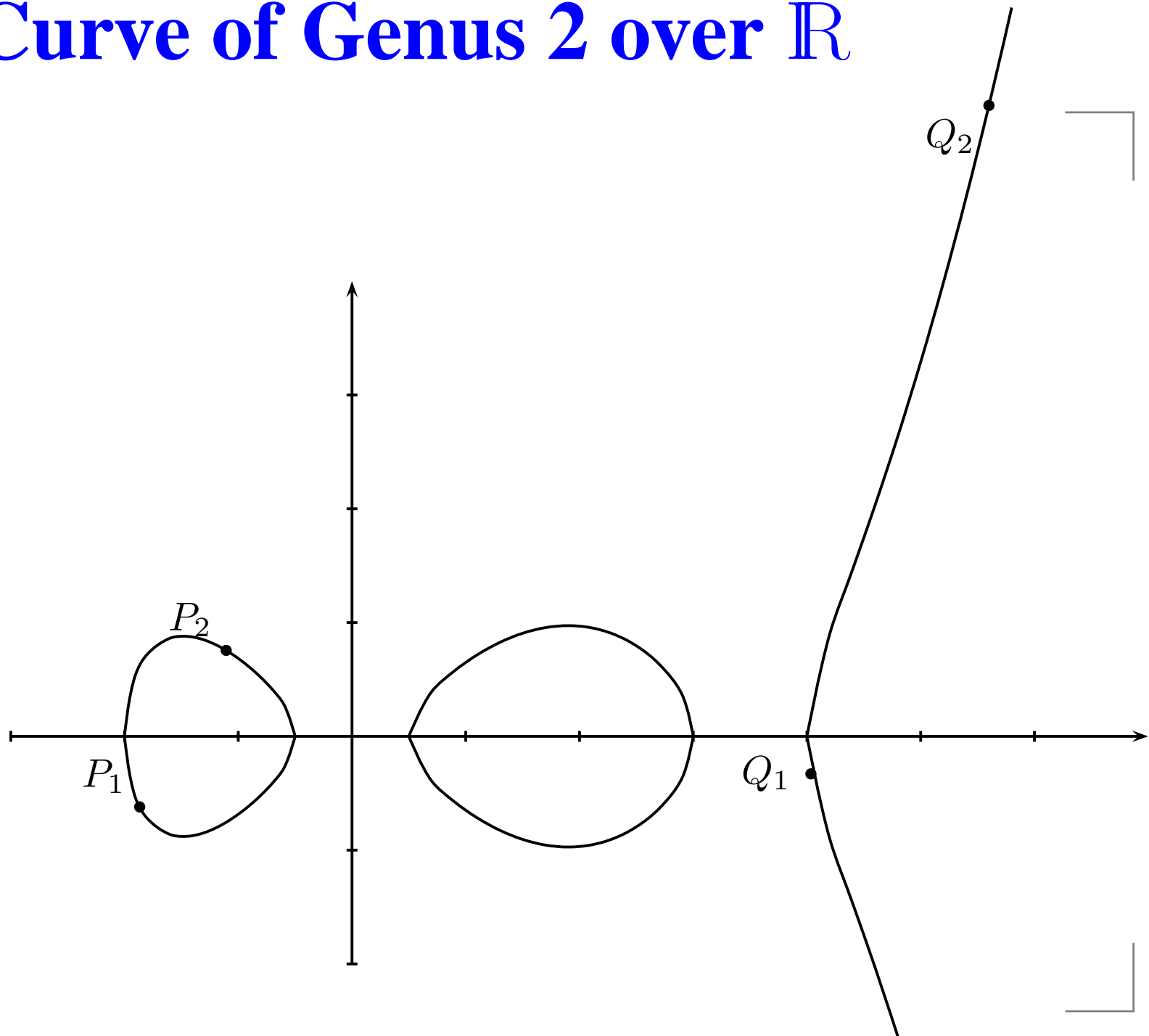
⇒ **divisor class group.**

$$\text{Pic}^0(C/\mathbb{F}_q) = \text{Div}^0(\mathbb{F}_q) / P(\mathbb{F}_q)$$

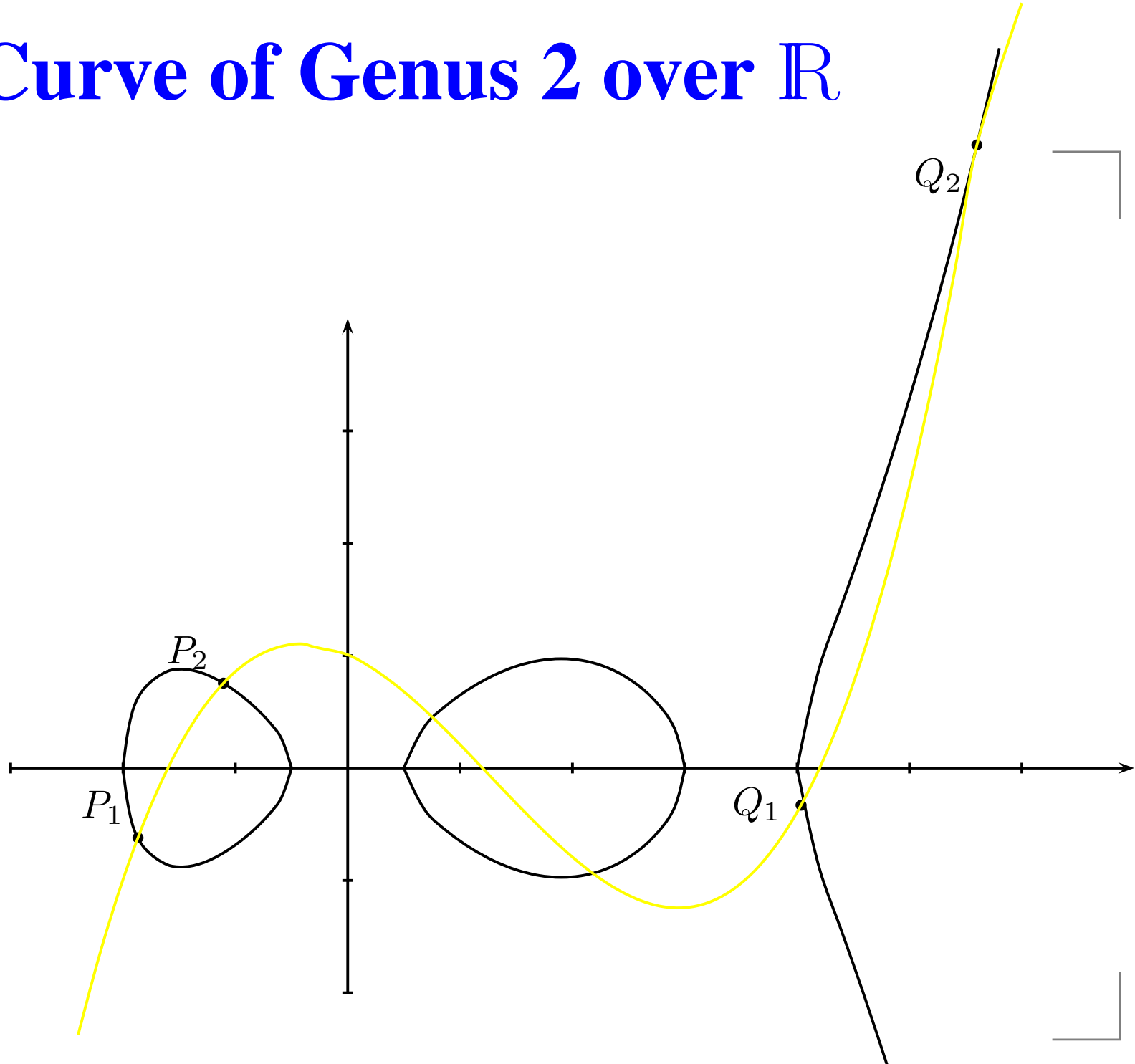
each class represented by degree zero divisor with $m \leq g$

$$\sum_{\substack{i=1 \\ P_i \in C \setminus \{\infty\}}}^m P_i - m\infty$$

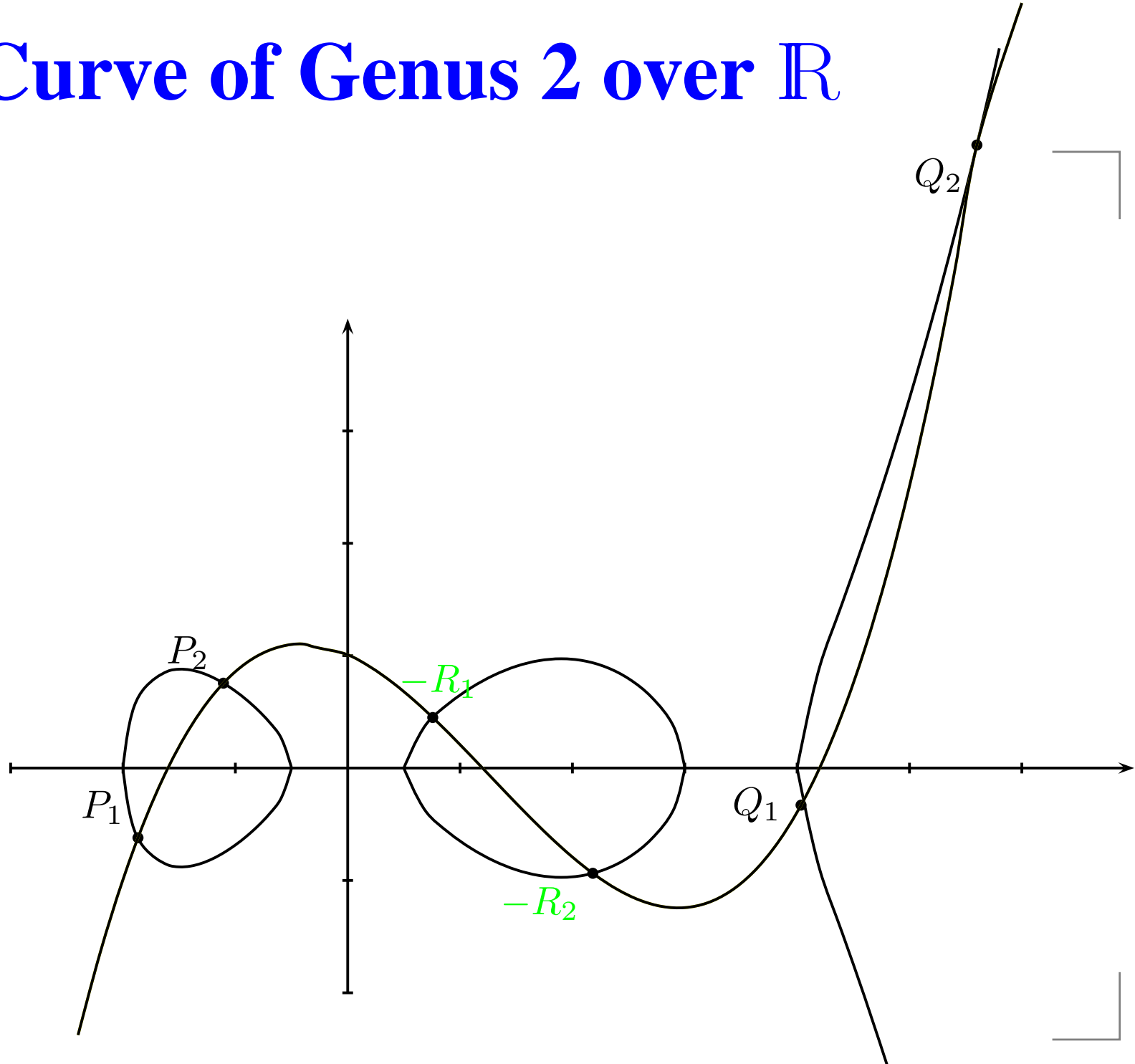
Curve of Genus 2 over \mathbb{R}



Curve of Genus 2 over \mathbb{R}

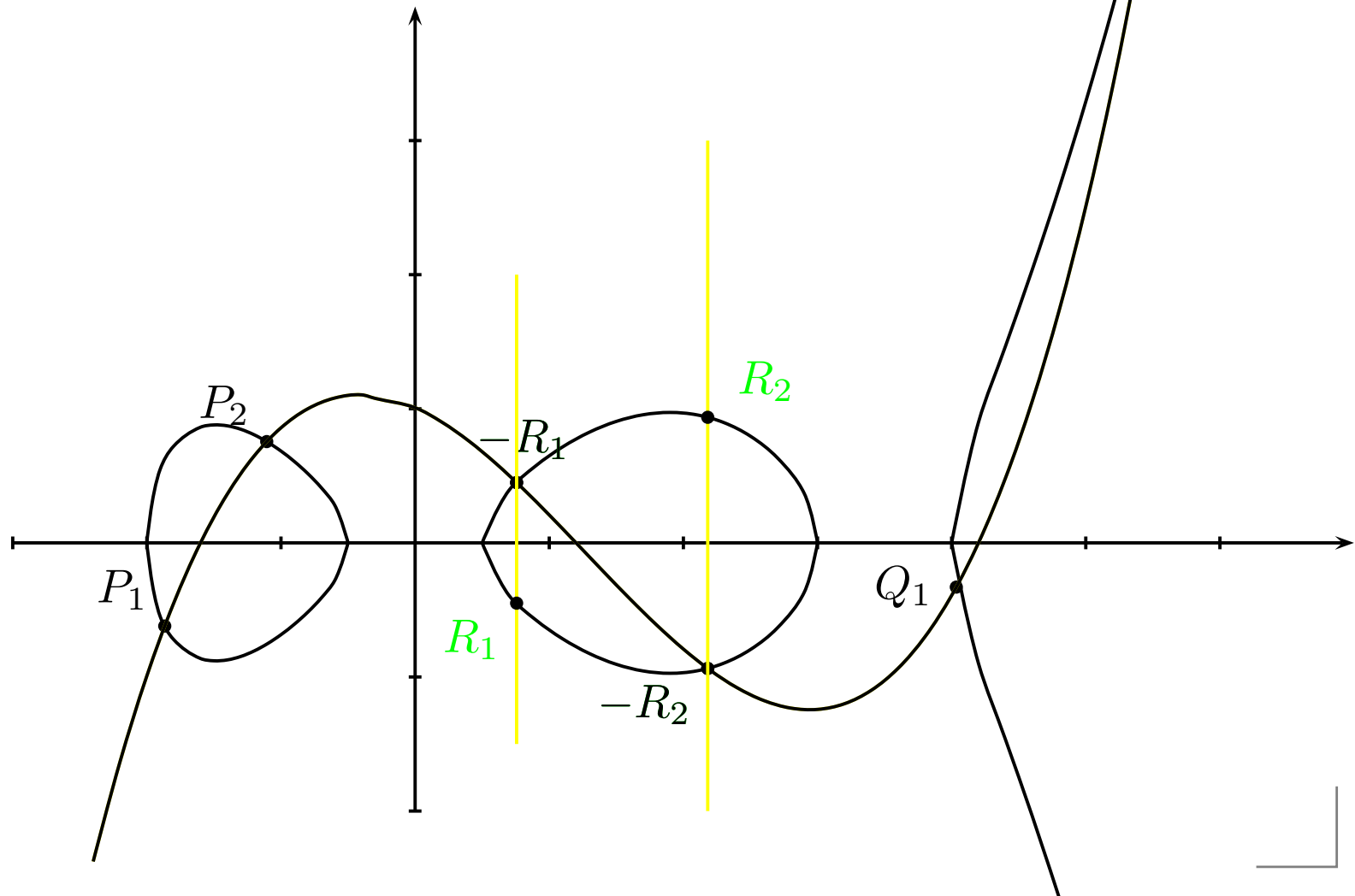


Curve of Genus 2 over \mathbb{R}



Curve of Genus 2 over \mathbb{R}

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



Mumford Representation

Divisor class group is isomorphic to
ideal class group $Cl(C/\mathbb{F}_q)$ 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, $\deg v < \deg u \leq g$, $u|v^2 + vh - f$.

\Rightarrow compact representation

isomorphism via

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

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 $d_1 = \gcd(u_1, u_2) = e_1u_1 + e_2u_2$
2. compute $d = \gcd(d_1, v_1 + v_2 + h) = c_1d_1 + c_2(v_1 + v_2 + h)$
3. let $s_1 = c_1e_1, s_2 = c_1e_2, s_3 = c_2$
4. $u = \frac{u_1u_2}{d^2} \quad v = \frac{s_1u_1v_2 + s_2u_2v_1 + s_3(v_1v_2 + f)}{d} \pmod{u}$
5. let $u' = \frac{f - vh - v^2}{u} \quad b' = (-h - v) \pmod{u'}$
6. if $\deg u' > g$ put $u := u', v := v'$ goto step 5
7. make u monic

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

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	<u>compute resultant r of u_1, u_2:</u> $z_1 = u_{11} - u_{21}, z_2 = u_{20} - u_{10}, z_3 = u_{11}z_1 + z_2;$ $r = z_2z_3 + z_1^2u_{10};$	1S, 3M
2	<u>compute almost inverse of u_2 modulo u_1 ($inv = r/u_2 \bmod u_1$):</u> $inv_1 = z_1, inv_0 = z_3;$	
3	<u>compute $s' = rs \equiv (v_1 - v_2)inv \bmod u_1$:</u> $w_0 = v_{10} - v_{20}, w_1 = v_{11} - v_{21}, w_2 = inv_0w_0, w_3 = inv_1w_1;$ $s'_1 = (inv_0 + inv_1)(w_0 + w_1) - w_2 - w_3(1 + u_{11}), s'_0 = w_2 - u_{10}w_3;$ if $s'_1 = 0$ see below	5M
4	<u>compute $s'' = x + s_0/s_1 = x + s'_0/s'_1$ and s_1:</u> $w_1 = (rs'_1)^{-1}(= 1/r^2s_1), w_2 = rw_1(= 1/s'_1), w_3 = s'^2_1w_1(= s_1);$ $w_4 = rw_2(= 1/s_1), w_5 = w^2_4, s''_0 = s'_0w_2;$	1, 2S, 5M
5	<u>compute $l' = s''u_2 = x^3 + l'_2x^2 + l'_1x + l'_0$:</u> $l'_2 = u_{21} + s''_0, l'_1 = u_{21}s''_0 + u_{20}, l'_0 = u_{20}s''_0$	2M
6	<u>compute $u' = (s(l + h + 2v_2) - k)/u_1 = x^2 + u'_1x + u'_0$:</u> $u'_0 = (s''_0 - u_{11})(s''_0 - z_1 + h_2w_4) - u_{10} + l'_1 + (h_1 + 2v_{21})w_4 + (2u_{21} + z_1 - f_4)w_5;$ $u'_1 = 2s''_0 - z_1 + h_2w_4 - w_5;$	3M
7	<u>compute $v' \equiv -h - (l + v_2) \bmod u' = v'_1x + v'_0$:</u> $w_1 = l'_2 - u'_1, w_2 = u'_1w_1 + u'_0 - l'_1, v'_1 = w_2w_3 - v_{21} - h_1 + h_2u'_1;$ $w_2 = u'_0w_1 - l'_0, v'_0 = w_2w_3 - v_{20} - h_0 + h_2u'_0;$	4M
total		1, 3S, 22M

Different Coordinates $g = 2$

affine \mathcal{A} :

$$D \sim [x^2 + u_1x + u_0, v_1x + v_0] \sim [u_1, u_0, v_1, v_0]$$

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
Upcoming paper by Roberto Avanzi (Essen), 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 $2\mathcal{N} = \mathcal{N}, \mathcal{N} + \mathcal{P} = \mathcal{N}$.
 - Implementation by Kim Nguyen (Philips) presented at ECC 2002 using \mathcal{P} is half as fast as elliptic
 - talk by Christof Paar (Bochum)

Speed-up via endomorphisms

Koblitz curves

Koblitz curves (subfield curves)

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

hyperelliptic curve with

$h(x), f(x) \in \mathbb{F}_q[x]$, q **small**

consider curve over \mathbb{F}_{q^n}

Example:

$$C : y^2 + xy = x^5 + x^2 + 1$$

hyperelliptic curve of genus 2 over \mathbb{F}_2

hyperelliptic curve of genus 2 over \mathbb{F}_{2^n}

History: Koblitz '89; Günther, L., Stein '00; L. 01 (Ph.D.)

Frobenius endomorphism σ :

$$P = (a, b) \in C(\mathbb{F}_{q^n})$$

$$\Rightarrow \sigma(P) := (a^q, b^q) \in C(\mathbb{F}_{q^n})$$

Normal basis

Basis of $\mathbb{F}_{q^n} = \{\theta, \theta^q, \theta^{q^2}, \dots, \theta^{q^{n-1}}\}$

Element $d \in \mathbb{F}_{q^n}$ represented by

$$d = (d_0, d_1, \dots, d_{n-1}), \quad d_i \in \mathbb{F}_q$$

$$d^q = (d_{n-1}, d_0, d_1, \dots, d_{n-2})$$

Remark: d^q realized by **cyclic shifting**,

q -th power also fast in polynomial basis

Frobenius endomorphism on $\text{Cl}(C/\mathbb{F}_q)$

Operation on ideal classes $D = [u(x), v(x)]$

$$\sigma(D) = [\sigma(u(x)), \sigma(v(x))],$$

where $\sigma(\sum d_i x^i) = \sum d_i^q x^i$.

Execution of Frobenius endomorphism takes at most $2g$ cyclic shiftings in normal basis representation (L., Nöcker: polynomial basis still faster)

Example:

C curve of genus 2 defined over \mathbb{F}_2

$$D = [x^2 + u_1x + u_0, v_1x + v_0] \quad \sigma(D) = [x^2 + u_1^2x + u_0^2, v_1^2x + v_0^2]$$

Characteristic polynomial of σ

$$P(T) = T^{2g} + a_1 T^{2g-1} + \dots + a_g T^g + \dots + a_1 q^{g-1} T + q^g$$

integer coefficients, degree $2g$

Examples for genus 2 over \mathbb{F}_2

Equation of C	$P(T)$
$v^2 + v = u^5 + u^3$	$T^4 + 2T^3 + 2T^2 + 4T + 4$
$v^2 + v = u^5 + u^3 + 1$	$T^4 - 2T^3 + 2T^2 - 4T + 4$
$v^2 + v = u^5 + u^3 + u$	$T^4 + 2T^2 + 4$
$v^2 + uv = u^5 + 1$	$T^4 + T^3 + 2T + 4$
$v^2 + uv = u^5 + u^2 + 1$	$T^4 - T^3 - 2T + 4$
$v^2 + (u^2 + u + 1)v = u^5 + u^4 + u^3$	$T^4 + T^2 + 4$
$v^2 + (u^2 + u)v = u^5 + u^4 + u$	$T^4 - T^2 + 4$
$v^2 + (u^2 + u + 1)v = u^5 + u^4$	$T^4 + 2T^3 + 3T^2 + 4T + 4$
$v^2 + (u^2 + u + 1)v = u^5 + u^4 + 1$	$T^4 - 2T^3 + 3T^2 - 4T + 4$

$P(T)$ **easy** to compute for **Koblitz curves**

Consequences I

$$-q^g D = \sigma^{2g}(D) + a_1 \sigma^{2g-1}(D) + \cdots + a_{2g-1} \sigma(D)$$

for $D \in \mathbf{Cl}(C/\mathbb{F}_q)$.

$$c = c_1 + c_2 \tau + \cdots + c_{2g} \tau^{2g-1} \in \mathbb{Z}[\tau]$$

$$\tau | c \Leftrightarrow q^g | c_1$$

Necessary for expansion: set of coefficients

$$R \supseteq \{0, \pm 1, \dots, \pm \lceil \frac{q^g - 1}{2} \rceil\}$$

Note:

Taking negative is for free.

$$D = [u(x), v(x)] \Rightarrow -D = [u(x), -h(x) - v(x)]$$

Consequences II

To compute $mD = \sum u_i \sigma^i(D)$ use **τ -adic expansion**

$$m = \sum u_i \tau^i,$$

where τ complex root of $P(T)$, $u_i \in R$: **set of coefficients.**

Results:

- if finite, expansions have length $\sim n$
- if not finite, then periodic with short period
- periodic expansions can easily be avoided

Comparison

Operations in **binary** representation:

$$\sim \frac{3}{2} g n \log_2 q \geq \frac{3}{2} g n$$

Operations in τ -**adic** representation:

- $(q^g - 2)/2$ precomputations

$$\sim \frac{q^g - 1}{q^g} n < n$$

- $(q^g - 1)q^g/2$ precomputations

$$\sim \frac{q^g - 1}{2q^g - 1} n < \frac{1}{2} n$$

Comparison

$q = 2$ same number of precomputations as signed binary

g	binary window	τ -adic $w = 1$	speed-up	binary window	τ -adic $w = 2$	speed-up
2	$11/4n$	$3/4n$	11/3	$31/12n$	$3/7n$	~ 6
3	$31/8n$	$7/8n$	31/7	$573/160n$	$7/15n$	~ 7.6
4	$79/16n$	$15/16n$	79/15	$1023/224n$	$15/31n$	~ 9.4

$q = 5$ comparison friendly towards ordinary curves

g	w_{bin}	binary window	τ -adic $w = 1$	speed-up	w_{bin}	binary window	τ -adic $w = 2$	speed-up
2	4	$47/8n$	$24/25n$	~ 6	9	$6n$	$24/49n$	~ 12
3	7	$511/64n$	$\sim n$	~ 8	13	$8n$	$124/249n$	~ 16
4	9	$10n$	$\sim n$	~ 10	18	$10n$	$\sim 1/2n$	~ 20

Generalized GLV

Other endomorphisms – GLV

- Gallant, Lambert, and Vanstone
- Park, Jeong, Kim, and Lim
- Sica, Ciet, and Quisquater

ϕ endomorphism of C , $P_\phi(T)$ characteristic polynomial of ϕ ,
 $d = \deg P_\phi \leq 2g$, l group order.

split

$$m = m_0 + m_1\phi + \cdots + m_{d-1}\phi^{d-1}, |m_i| \sim l^{1/d}$$

for $d = 2$ use joint-sparse form (JSF) of exponent,
otherwise interleaved multiplications.

Both significantly faster than binary method

Combination of GLV and expansion

Ciet, L., Sica, Quisquater, Eurocrypt '03

ϕ satisfies

$$T^2 + rT + s$$

use GLV

$$m = m_0 + m_1\phi, \quad |m_i| \sim l^{1/2}$$

expand

$$m_0 + m_1\phi = k_0 + k_1\phi + k_2\phi^2 + \dots, \quad k_i \in \mathcal{R}, \text{length} \sim \log_s m$$

precompute $r_i P$ for $r_i \in \mathcal{R} = \{0, \pm 1, \dots, \lceil (s-1)/2 \rceil\}$

together with ϕ -JSF \Rightarrow further speed-up if computation of

$\phi(P)$ less expansive than s -fold

Trace zero variety

Trace-zero subvariety

genus 1 or 2 curve defined over \mathbb{F}_p , considered over \mathbb{F}_{p^n} ,
where $n \in \{3, 5\}$ for $g = 1$ and $n = 3$ for $g = 2$
trace zero property

$$D \in G \Leftrightarrow D \in \text{Cl}(C/\mathbb{F}_{p^n}) \text{ and } D + \sigma(D) + \cdots + \sigma^{n-1}(D) = 0,$$

subgroup of $\text{Cl}(C/\mathbb{F}_{p^n})$

('Koblitz curves' for small extension)

History: Frey '98, Naumann '99 ($g = 1$),
L. '01 ($g = 2$), Blady '02 ($g = 1$)
Silverberg/Rubin '02 (supersingular curves)
Avanzi, Diem, Frey, L., Scholten '03

Background

dimension $(n - 1)g$, group size from $P(T)$,

$$\#G \sim \#\mathbf{Cl}(C/\mathbb{F}_{p^n})/\#\mathbf{Cl}(C/\mathbb{F}_p) \sim p^{(n-1)g}$$

Theorem Put $g = 2, n = 3$. Let $2, 3 \nmid l \mid \#\mathbf{Cl}(C/\mathbb{F}_{p^3})$. The nontrivial elements in the subgroup of order l of the trace zero variety G are the divisor classes represented by

$$P_1 + P_2 - 2\infty \notin \text{Div}(C/\mathbb{F}_p)^0,$$

where $P_1 \neq P_2, \sigma(P_2), \sigma^2(P_2)$.

Scalar multiples in G

Frobenius endomorphism satisfies characteristic polynomial

$$P(T) = T^2 + a_1T + p \text{ resp. } P(T) = T^4 + a_1T^3 + a_2T^2 + a_1pT + p^2.$$

and trace relation

$$T^2 + T + 1 \text{ resp. } T^4 + T^3 + T^2 + T + 1$$

instead of computing mD for $0 \leq m < l$, $l \sim p^{(n-1)g}$ group
order $\langle D \rangle \subseteq G$ use

$$r_0D + \cdots + r_{n-2}\sigma(D), \quad |r_i| \sim \sqrt[n]{m}.$$

and (pairwise) Joint Sparse Form (JSF) of r_i .

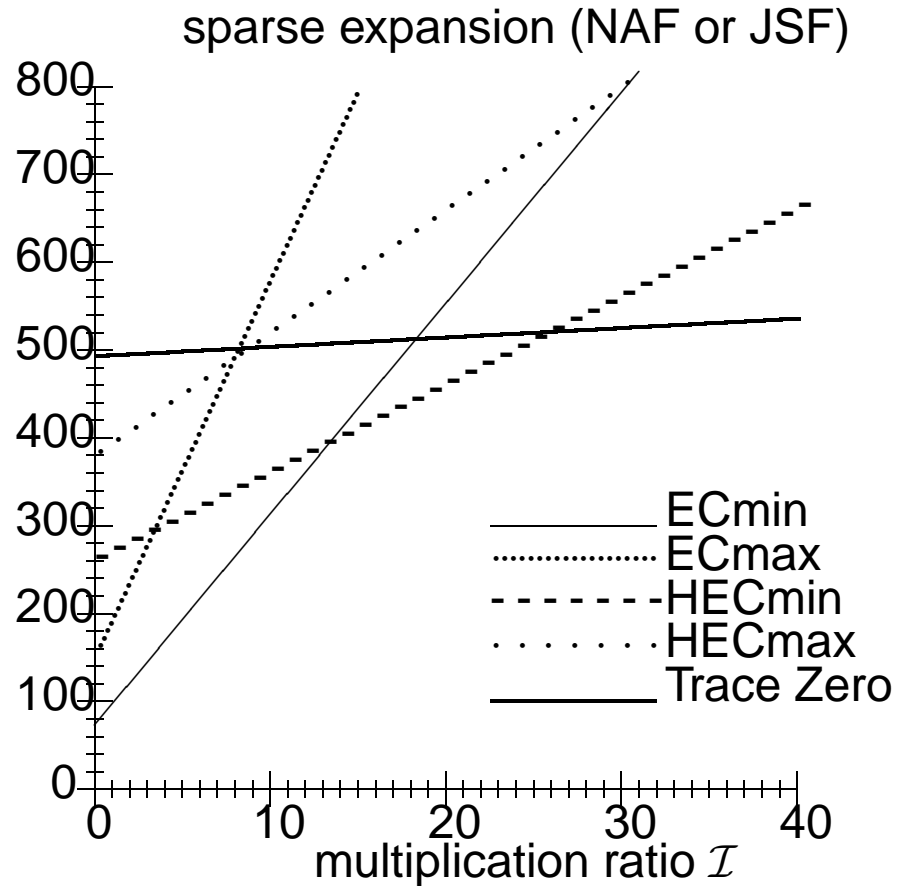
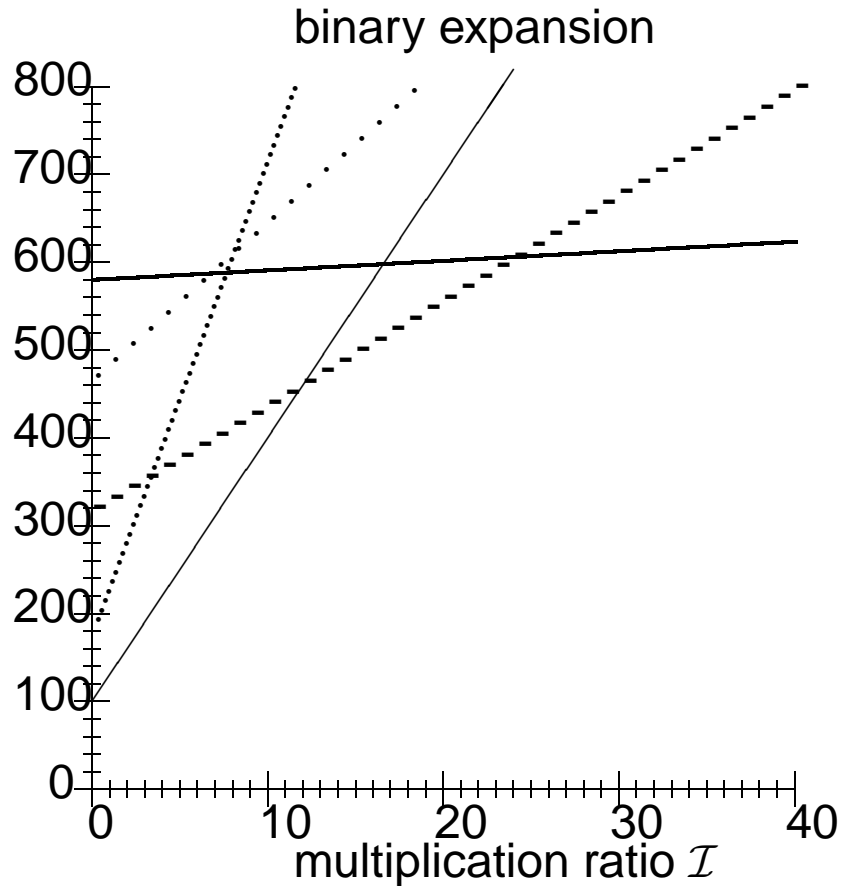
Comparison I, $g = 2, n = 3$

	Elliptic, in $\mathbb{F}_{p''}$			Genus 2, in $\mathbb{F}_{p'}$			$G (g = 2)$, in \mathbb{F}_p		
	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.
Add.	1	1	2	1	3	22	1	21	141
Doub.	1	2	2	1	5	22	1	33	141
m -fold	6λ	10λ	12λ	6λ	26λ	132λ	3.5λ	97.5λ	501.5λ
NAF/ JSF	4.8λ	8.8λ	9.6λ	4.8λ	22.4λ	105.6λ	3λ	87λ	423λ

using efficient arithmetic in \mathbb{F}_{p^3}

(NAF includes same number of precomputations)

Comparison II, $g = 2, n = 3$



Implementation: work in progress by Avanzi, L.

The End

The END

Thanks!