Cryptographic Applications of Trace Zero Varieties

Tanja Lange

ITSC - Information-Security and Cryptography

Ruhr-University of Bochum

lange@itsc.ruhr-uni-bochum.de

09.10.2003

credits to Avanzi, Frey, Frobenius

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)

This talk

Elliptic curves (genus $g = 1$)

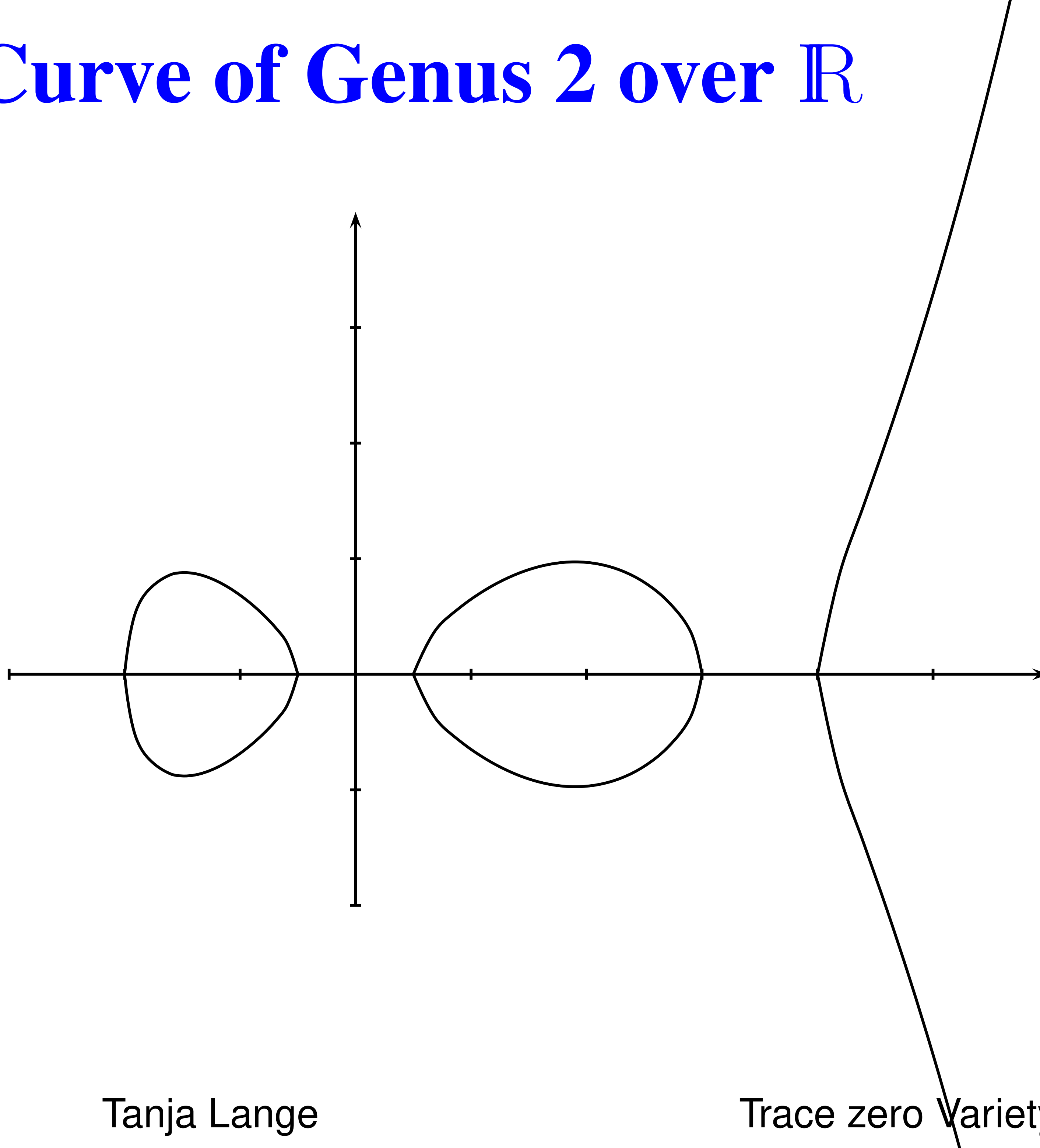
$$y^2 = x^3 + a_4 x + a_6$$

Curves of genus $g = 2$

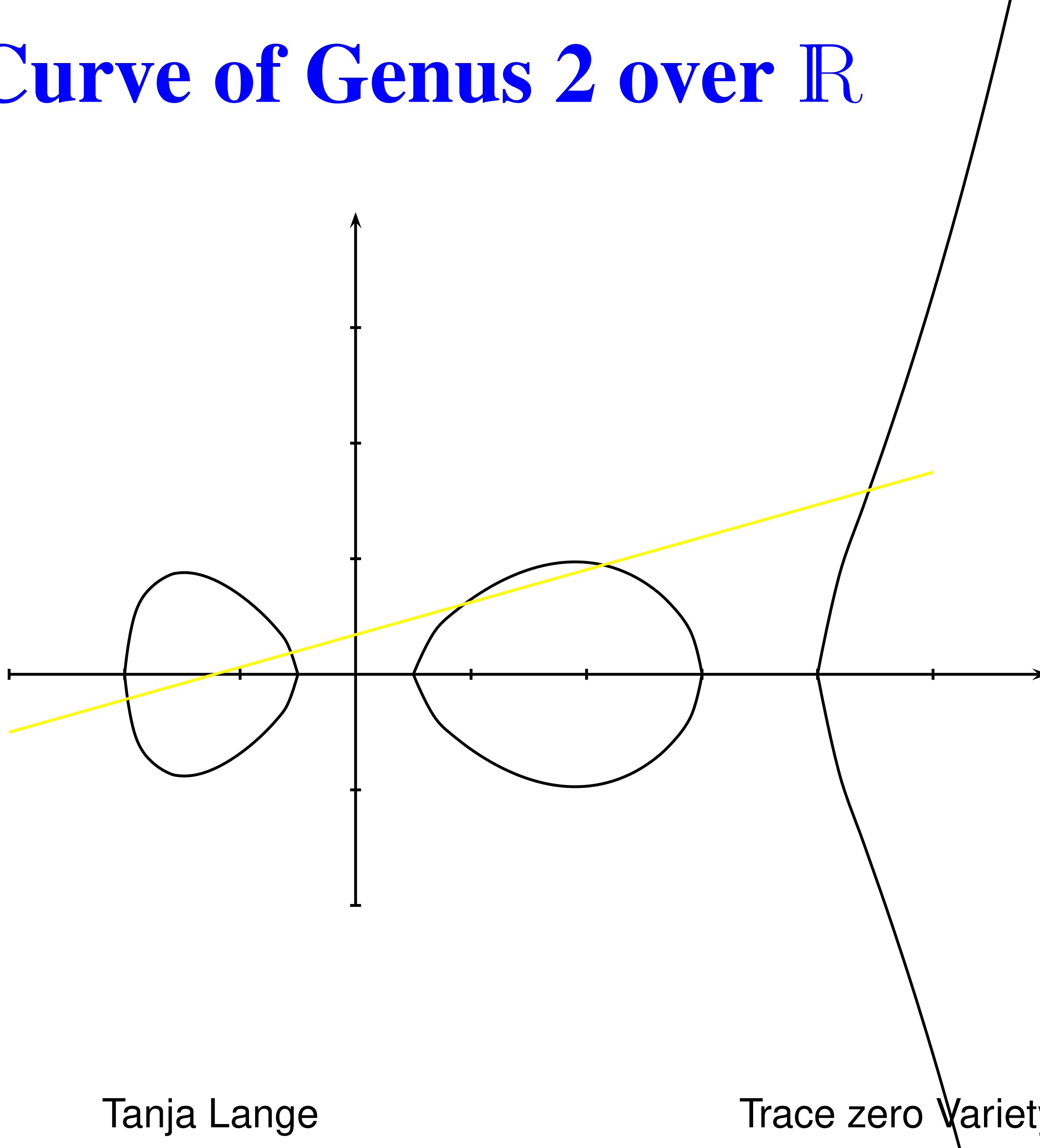
$$y^2 = x^5 + f_3 x^3 + f_2 x^2 + f_1 x + f_0$$

fields of odd characteristic $\mathbb{F}_{p^n}, p$ prime

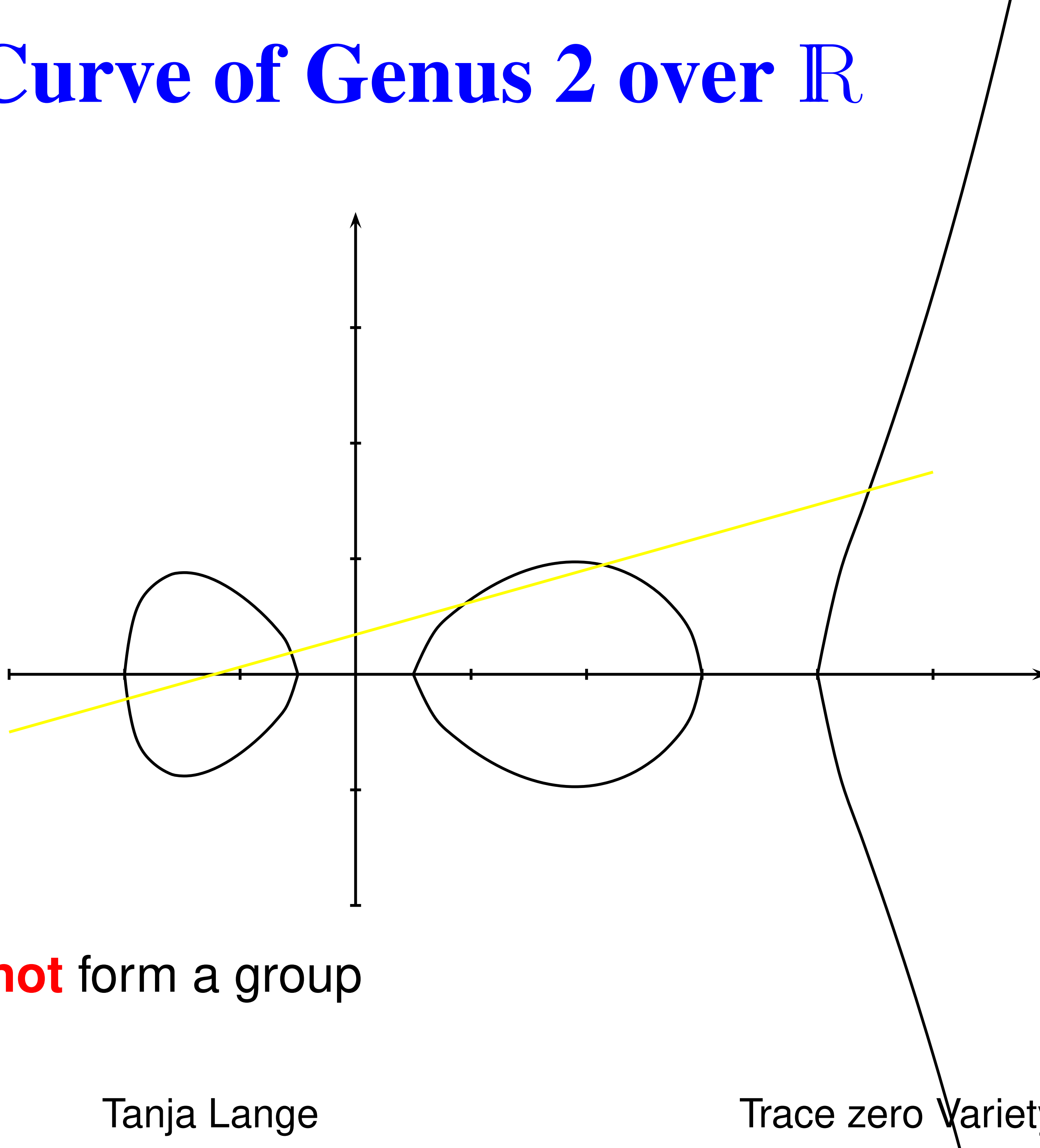
Curve of Genus 2 over $\mathbb{R}$



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 (divisors arising from functions):

Divisor Class Group

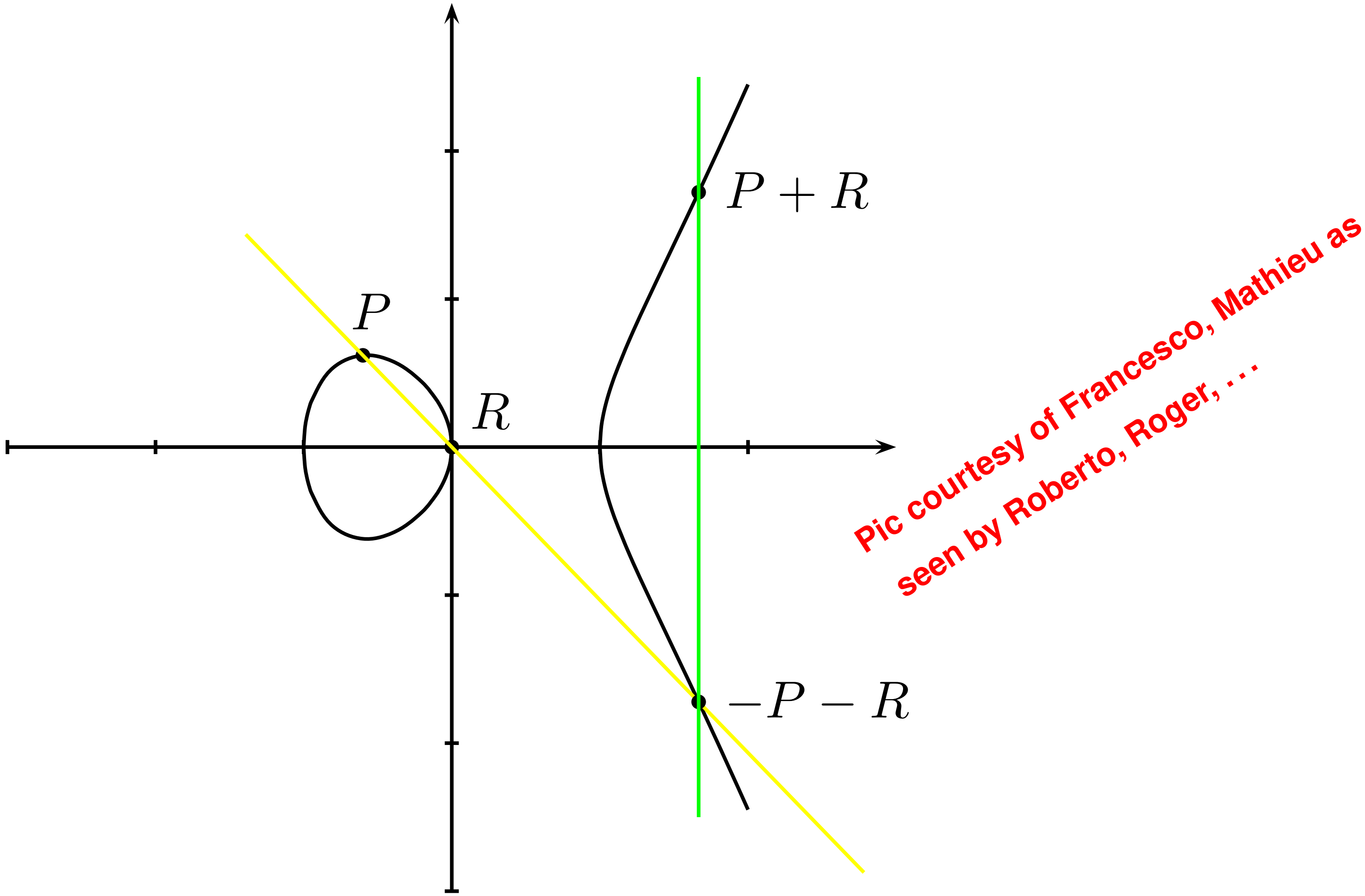
$$\mathrm{Pic}^0(C/\mathbb{F}_q) = Div^0(\mathbb{F}_q)/P(\mathbb{F}_q)$$

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

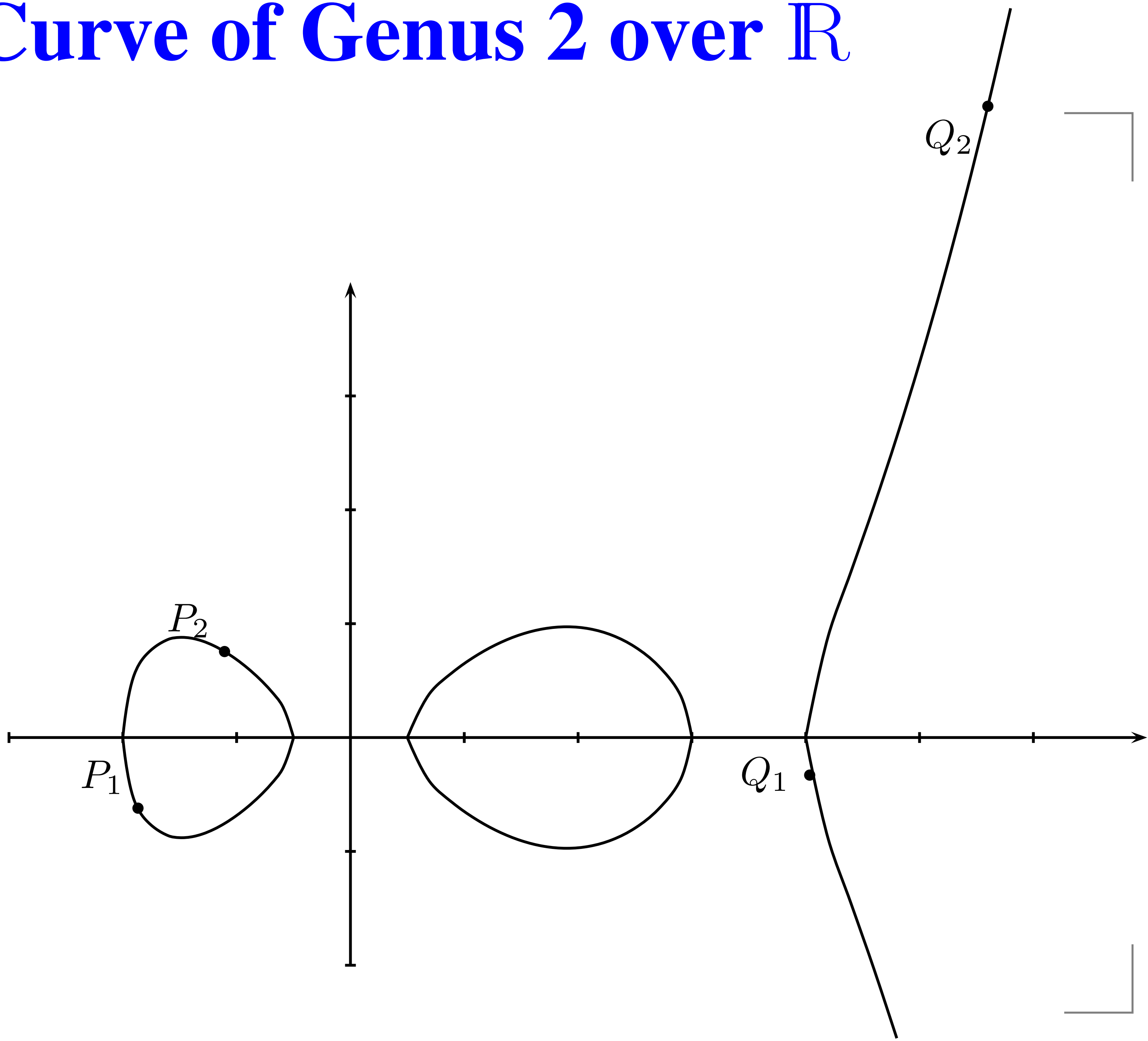
$$\sum_{\substack{i=1 \\ P_i \in C \setminus \{\infty\}}}^{m} P_i - m\infty$$

. . . and now to something completely different . . .

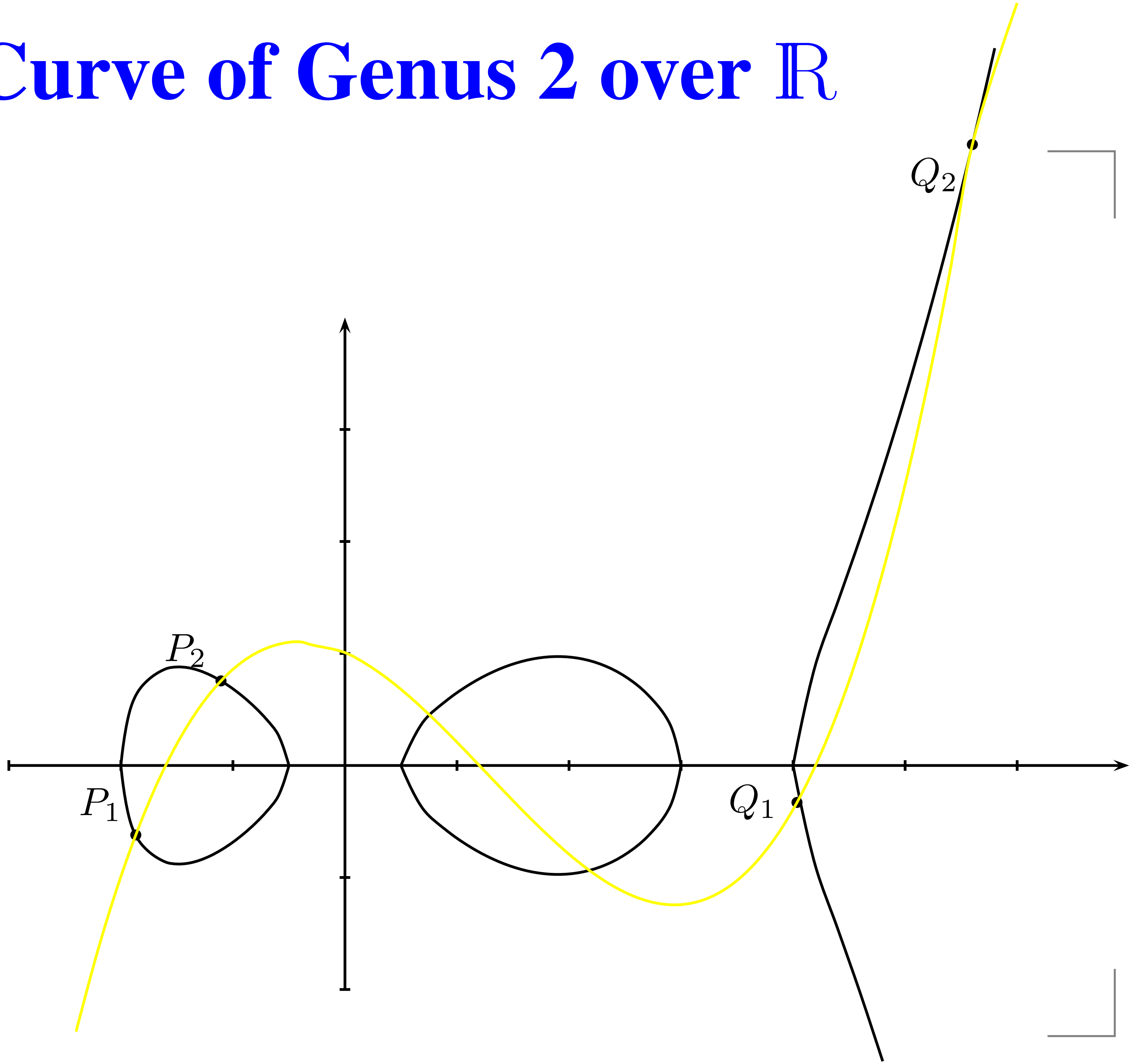
Elliptic Curve over $\mathbb{R}$



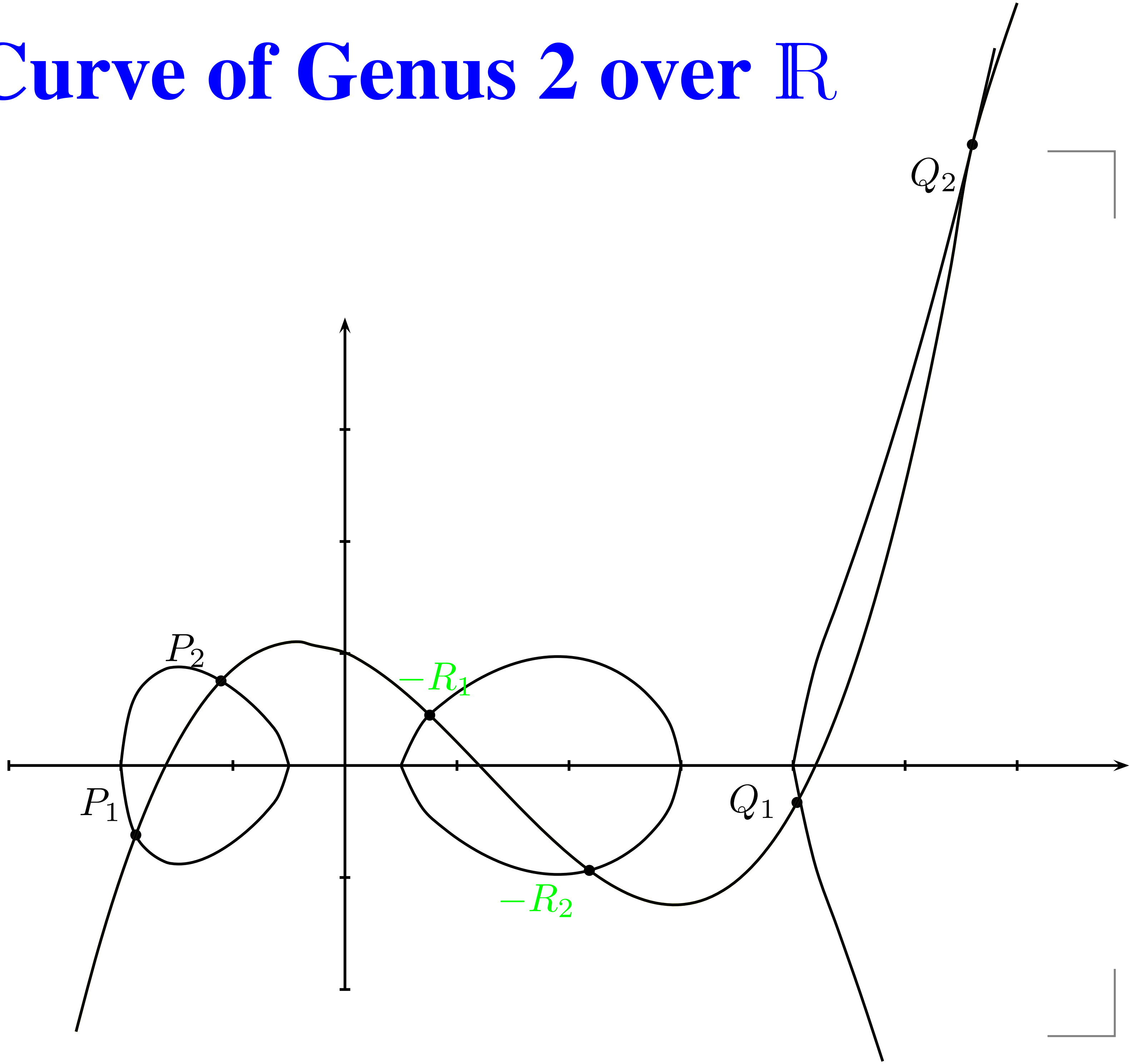
Curve of Genus 2 over $\mathbb{R}$



Curve of Genus 2 over $\mathbb{R}$

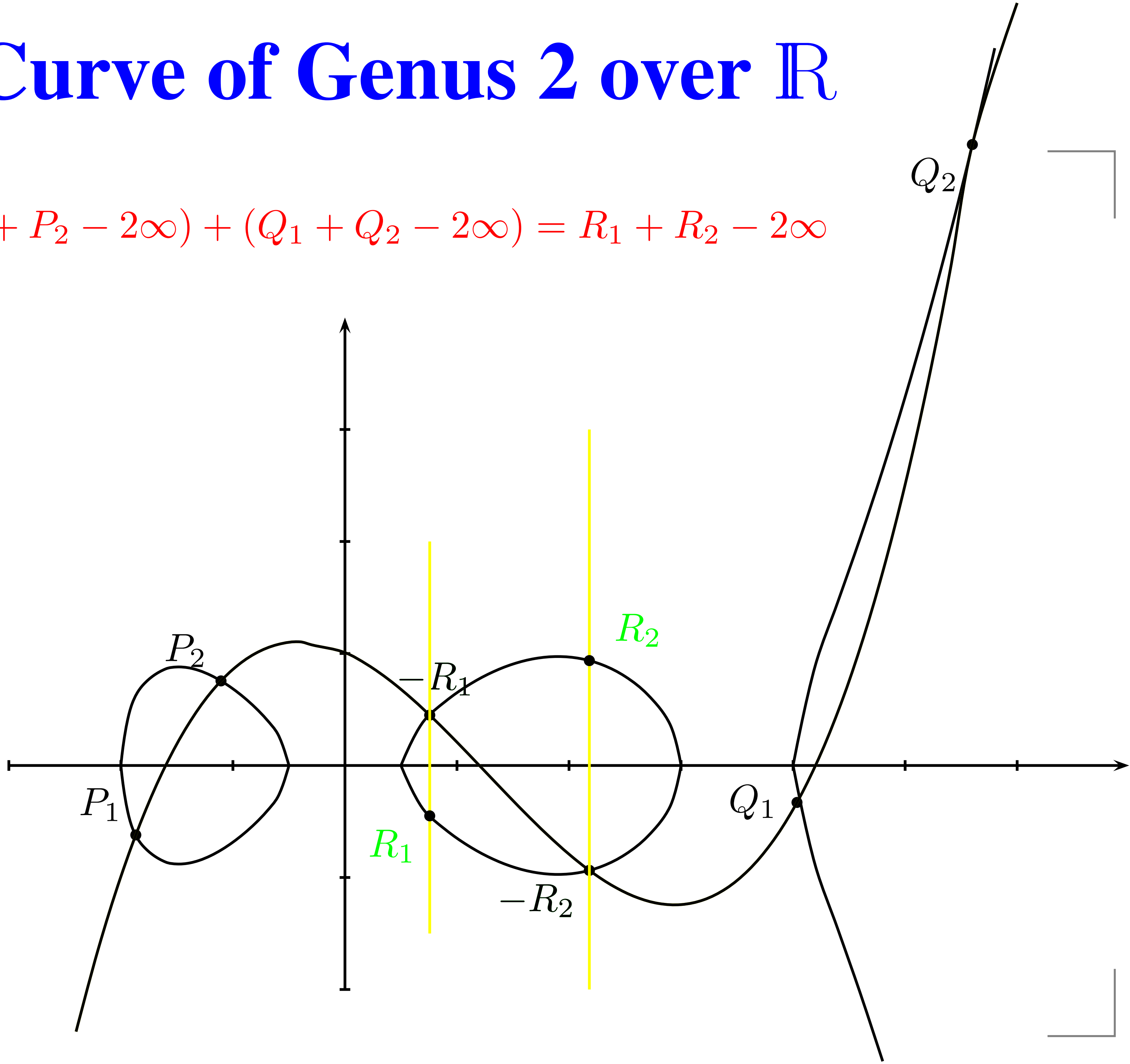


Curve of Genus 2 over $\mathbb{R}$



Curve of Genus 2 over $\mathbb{R}$

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



this is the most common case

– both divisors consist of $g = 2$ points

Mumford Representation

uses

$$\mathrm{Pic}^0(C/\mathbb{F}_q) \cong \mathbf{Cl}(C/\mathbb{F}_q)$$

representation

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

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

isomorphism

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

arithmetic uses $[u, v]$ only

Koblitz curves (subfield curves)

Frobenius alone again?

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

hyperelliptic curve with
$h(x), f(x) \in \mathbb{F}_p[x]$, p **small**
consider curve over $\mathbb{F}_{p^n}$

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

Frobenius endomorphism on $\mathbf{Cl}(C/\mathbb{F}_{p^n})$

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 is much faster than one group operation

Characteristic polynomial

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

integer coefficients, degree $2g$

Trace Zero Subgroup G

use idea of Koblitz curves with a small extension $n = 3, 5$ (should be prime) and large enough p

Subgroups:

- $\{D | \sigma(D) = D\}$ ideal class group $\mathbf{Cl}(C/\mathbb{F}_p)$
- $\{D | \sigma^{n-1}(D) + \sigma^{n-2}(D) + \cdots + \sigma(D) + D = 0\} =: G$

obviously these are groups, security see next talk

Trace-zero subvariety

genus 1 or 2 curve defined over $\mathbb{F}_p$, considered over $\mathbb{F}_{p^n}$, where

$$n \in \{3, 5\} \text{ for } g = 1$$

$$n = 3 \text{ for } g = 2$$

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

Avanzi, Diem, Frey, L., Scholten '03

Geometric construction I

Example: elliptic curve

$$y^2 = x^3 + Ax + B \text{ over } \mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$$

write $x = \sum_{i=0}^{n-1} x_i\alpha^i$, $y = \sum_{i=0}^{n-1} y_i\alpha^i$

sort according to powers of α

$\Rightarrow$ n-dimensional variety over $\mathbb{F}_p$.

in general $\Rightarrow$ ng-dimensional variety over $\mathbb{F}_p$.

Geometric construction II

Trace condition (broken down to this g-dimensional variety over $\mathbb{F}_p$) cuts out subvariety $\mathcal{G}$

- $\mathcal{G}$ isomorphic to G (as groups)
- $\dim \mathcal{G} = n - 1$.
- group size computable from $P(T)$

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

Representations $g = 2$

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

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

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

Scalar multiples in G

Frobenius endomorphism satisfies characteristic polynomial

$P(T) = T^2 + a_1 T + p$ resp. $P(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 p T + p^2$.

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 oder $\langle D \rangle \subseteq G$ use

$$r_0 D + \cdots r_{n-2} \sigma(D), \ |r_i| \sim \sqrt[n]{m}.$$

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

Joint Sparse Form (JSF)

- (JSF 1) Of any three consecutive columns at least one is a zero column.
- (JSF 2) It is never the case that $u_{i,j+1}u_{i,j} = -1$.
- (JSF 3) If $u_{i,j+1}u_{i,j} \neq 0$ then $u_{1-i,j+1} = \pm 1$ and $u_{1-i,j} = 0$.

Example: $k_0 = 403, k_1 = 334$

$$\begin{array}{lcl} k_0 & = & \langle\ 1\ \ 0\ \ \text{-1}\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ \text{-1}\ \rangle \\ k_1 & = & \langle\ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ \text{-1}\ \ 0\ \rangle \end{array}$$

$$\begin{array}{lcl} k_0 & = & \langle\ 1\ \ 0\ \ \text{-1}\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \rangle \\ k_1 & = & \langle\ 1\ \ 0\ \ \text{-1}\ \ \text{-1}\ \ 0\ \ 1\ \ 0\ \ 0\ \ \text{-1}\ \ 0\ \rangle \end{array}$$

Avoid collisions I

Theorem

C elliptic curve over $\mathbb{F}_p$, $P(T) = T^2 + a_1 T + p$. D generator of subgroup of prime order l in trace zero variety G for $n = 3$.

$$\mathbf{r} := \min\{\frac{l}{p - a_1}, \frac{p-1}{\gcd(p-1, a_1 - 1)}\}.$$

The $\mathbf{r}^2$ classes $r_0 D + r_1 \sigma(D),\ 0 \le r_i < \mathbf{r}$ are distinct.

Avoid collisions II

Theorem

C genus 2 hyperelliptic curve over $\mathbb{F}_p$,
$P(T) = T^4 + a_1T^3 + a_2T^2 + a_1pT + p^2$. D generator of subgroup of prime order l in trace zero variety G.

$$\mathbf{r} := \min\left\{\left\lfloor\frac{l}{m}\right\rfloor, \frac{p^2 - a_2 + a_1}{\gcd(p^2 - a_2 + a_1, a_1p - a_2 + 1)}\right\},$$

where $m = \max\{p^2 + a_1p - 2a_2 + a_1 + 1, p^2 + a_1 - a_1p - 1\}$.
The $\mathbf{r}^2$ classes $r_0D + r_1\sigma(D),\ 0 \le r_i < \mathbf{r}$ are distinct.

Alternative

Use $P(T)$ to expand given integer m
– here $g = 1, n = 3$

$$
\begin{aligned}
m &= n_0 + ((m - n_0)/p)(-a_1 T - T^2) \\
&= n_0 + \frac{m - n_0}{p}(-a_1 T - T^2) \\
&= n_0 + n_1 T + \frac{-a_1 \frac{m-n_0}{p} - n_1}{p}(-a_1 T^2 - T^3) - \frac{m - n_0}{p} T^2
\end{aligned}
$$

we might be done

$$|a_1| < 2\sqrt{p}, \quad p > 5$$
$$\Rightarrow (-a_1(m-n_0)/p - n_1)/p \leq 2\sqrt{p}$$
$$\Rightarrow (a_1^2(m-n_0)/p + a_1 n_1 - m + n_0)/p < 4p + 2.$$

$$\begin{aligned} m_0 &= n_0 + (n_1(1-a_1) + m - n_0)/p + a_1(1-a_1)(m-n_0)/p^2 \\ m_1 &= n_1 + (-a_1 n_1 + m - n_0)/p - a_1^2(m-n_0)/p^2 \end{aligned}$$

Arithmetic in $\mathbb{F}_{p^3}$ I

$$
\begin{aligned}
(b_2\xi^2 + b_1\xi + b_0)(c_2\xi^2 + c_1\xi + c_0) = \\
&\big(b_1c_1 + (b_0+b_2)(c_0+c_2) - b_0c_0 - b_2c_2\big)\xi^2 \\
&+\big((b_0+b_1)(c_0+c_1) - b_0c_0 - b_1c_1 + b_2c_2\alpha\big)\xi \\
&+b_0c_0 + ((b_1+b_2)(c_1+c_2) - b_1c_1 - b_2c_2)\alpha.
\end{aligned}
$$

$$\Delta = b_2^3\alpha^2 + b_1^3\alpha + b_0^3 - 3b_0b_1b_2\alpha.$$

$$
\begin{aligned}
&(b_2\xi^2 + b_1\xi + b_0)^{-1} = \\
&((b_1^2 - b_2b_0)\xi^2 + (b_2^2\alpha - b_1b_0)\xi + b_0^2 - b_2b_1\alpha)/\Delta.
\end{aligned}
$$

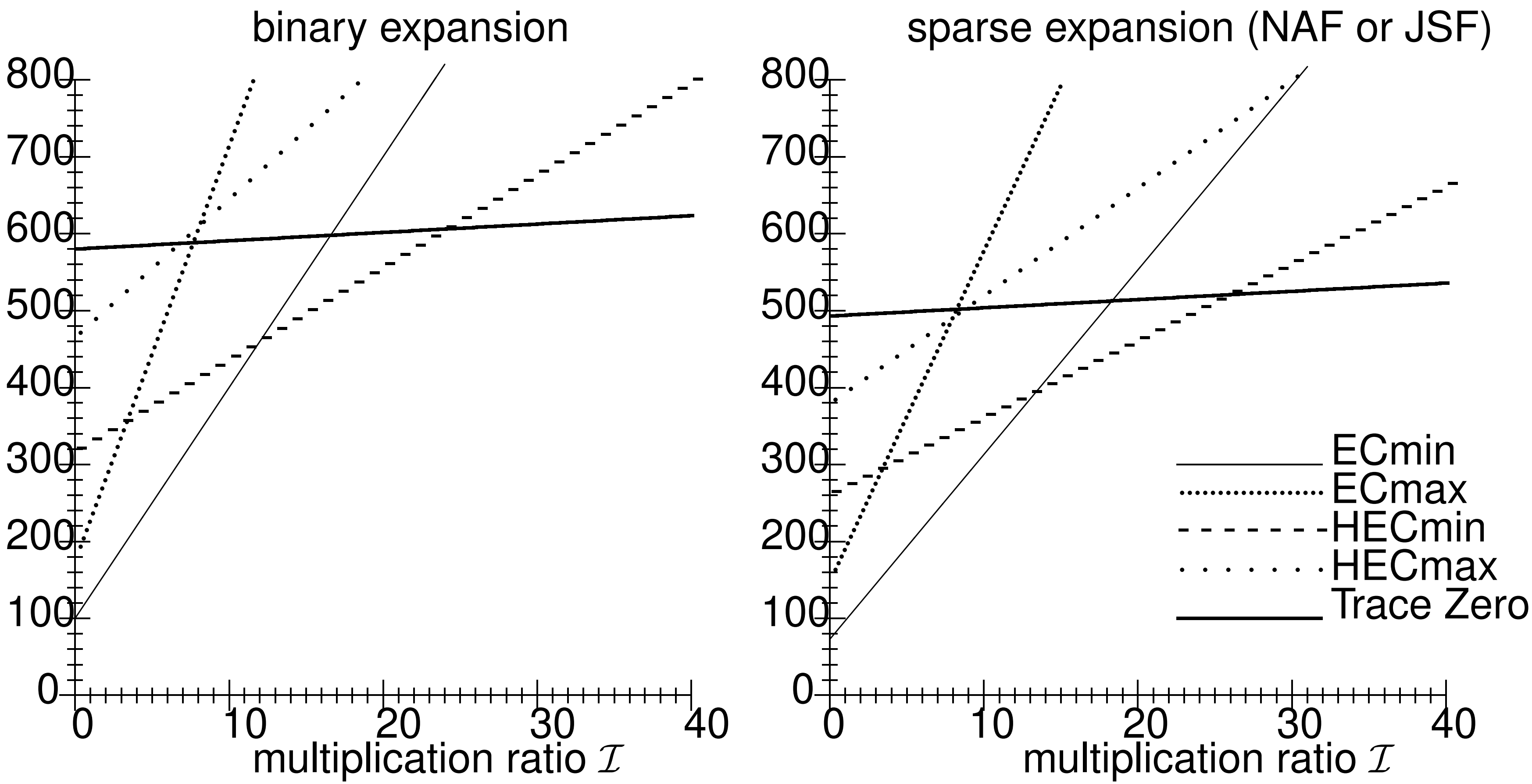
Comparison I, $g = 2, n = 3$

	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 – very preliminary ...

bits		$E/\mathbb{F}_{p'}$, $g = 1$	$\mathbf{Cl}(C/\mathbb{F}_{p''})$, $g = 2$	$G, n = 3$, $g = 1$	$G, n = 5$, $g = 1$	$G, n = 3$, $g = 2$
160	unsig.	1,6ms	1,71ms	1,48ms	1,3ms	3,18ms
	prec.			1,38ms	1,22ms	2,98ms
192	unsig.	2ms	2,1ms	1,94ms	1,76ms	3,7ms
	prec.			1,86ms	1,68ms	3,3ms
256	unsig.	–	4,4ms	4,3ms	2,74ms	5,86ms
	prec.			3,96ms	2,6ms	5,38ms

Open Problem

The End

The END

Thanks!