Hyperelliptic Curve Arithmetic

Renate Scheidler

UNIVERSITY OF CALGARY

12th International Conference on Finite Fields and Their Applications

July 16, 2015

Uses of Jacobian Arithmetic

- **Number Theory**
  - Invariant computation (class group/Jacobian, regulator, ...)
  - Function field construction
  - Function field tabulation
- **Geometry**
  - Algebraic curves
- **Cryptography**
  - Discrete log based crypto
  - Pairing based crypto
- **Coding Theory?**

Discrete Logarithm Based Cryptography

Groups that are used for discrete log based crypto should satisfy the following properties:

For practicality:

- Compact group elements
- Fast group operation

For security:

- Large order
- Cyclic or almost cyclic (plus some other restrictions on the order)
- Intractable discrete logarithm problem (DLP)

Suitable Groups

Proposed Groups:

- $G = \mathbb{F}_p^*$ (Diffie-Hellman 1976)
- Elliptic curves (Koblitz 1985, Miller 1985)
- Hyperelliptic curves (Koblitz 1989)

Fastest *generic* DLP algorithms: $O(\sqrt{|G|})$ group operations

- Best known for elliptic (i.e. genus 1) and genus 2 hyperelliptic curves
- Faster algorithms known for finite fields and higher genus curves

For curves of genus g over a finite field $\mathbb{F}_q$: $|G| \sim q^g$ as $q \to \infty$.

If we want 80 bits of security (i.e. $\sqrt{q^g} \approx 2^{80}$):

- $g = 1$: $q \approx 2^{160}$
- $g = 2$: $q \approx 2^{80}$ (slower group arithmetic but faster field arithmetic)

Elliptic Curves

Let K be a field (in crypto, $K = \mathbb{F}_q$ with q prime or $q = 2^n$)

Weierstraß equation over K:

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (*)$$

with $a_1, a_2, a_3, a_4, a_6 \in K$

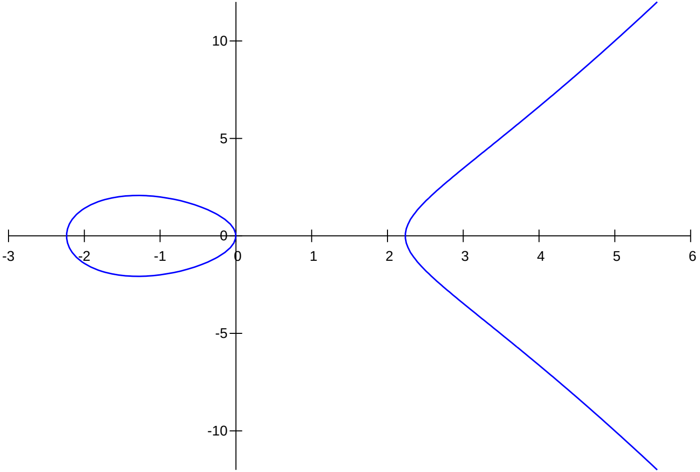
Elliptic curve: Weierstraß equation & non-singularity condition: there are no simultaneous solutions to $(*)$ and

$$\begin{aligned} 2y + a_1x + a_3 &= 0 \\ a_1y &= 3x^2 + 2a_2x + a_4 \end{aligned}$$

Non-singularity $\iff$ $\Delta \neq 0$ where Δ is the discriminant of E

An Example

$E: y^2 = x^3 - 5x$ over $\mathbb{Q}$



For char$(K) \neq 2, 3$, the variable transformations

$$y \to y - (a_1 x + a_3)/2, \text{ then } x \to x - (a_1^2 + 4a_2)/12$$

yield an elliptic curve in short Weierstraß form:

$$E \ : \ y^2 = x^3 + Ax + B \qquad (A, B \in K)$$

$$\text{Discriminant } \ \Delta = 4A^3 + 27B^2 \neq 0 \quad \text{(cubic in } x \text{ has distinct roots)}$$

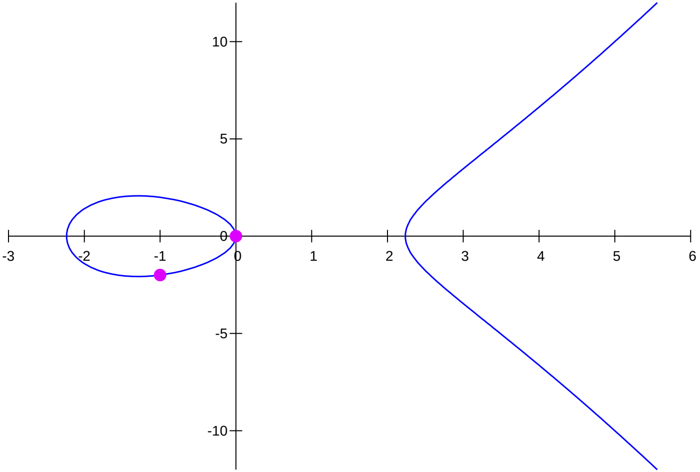
For any field L with $K \subseteq L \subseteq \overline{K}$:

$$E(L) \ = \ \{(x_0, y_0) \in L \times L \mid y_0^2 = x_0^3 + Ax_0 + B\} \cup \{\infty\}$$

set of L-rational points on E.

An Example

$P_1 = (-1, 2),\ P_2 = (0, 0) \in\ E(\mathbb{Q})$



The Mysterious Point at Infinity

In E, replace x by x/z, y by y/z, then multiply by z^3:

$$E_{\text{proj}} \ : \ y^2z = x^3 + Axz^2 + Bz^3 \ .$$

Points on E_{proj}:

$[x : y : z] \neq [0 : 0 : 0]$, normalized so the last non-zero entry is 1.

Affine Points		Projective Points
(x, y)	$\leftrightarrow$	$[x : y : 1]$
∞	$\leftrightarrow$	$[0 : 1 : 0]$

Arithmetic on E

Goal: Make $E(K)$ into an additive (Abelian) group:

- The identity is the point at infinity.
- The inverse of a point $P = (x_0, y_0)$ is its opposite $\overline{P} = (x_0, -y_0)^\dagger$

  †true for odd characteristic only; in general, the opposite of a point $P = (x_0, y_0)$ is $\overline{P} = (x_0, -y_0 - a_1x_0 - a_3)$.

By Bezout's Theorem, any line intersects E in three points.

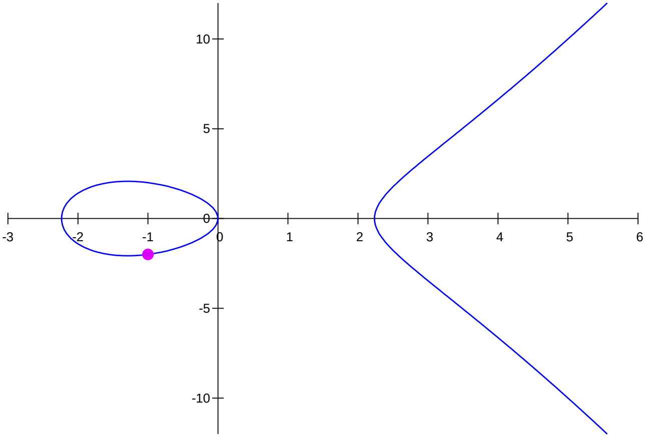
- Need to count multiplicities;
- If one of the points is ∞, the line is "vertical"†

  †true for odd characteristic only; in general, the line goes through P and $\overline{P}$.

Motto: "Any three collinear points on E sum to zero (i.e. ∞)."

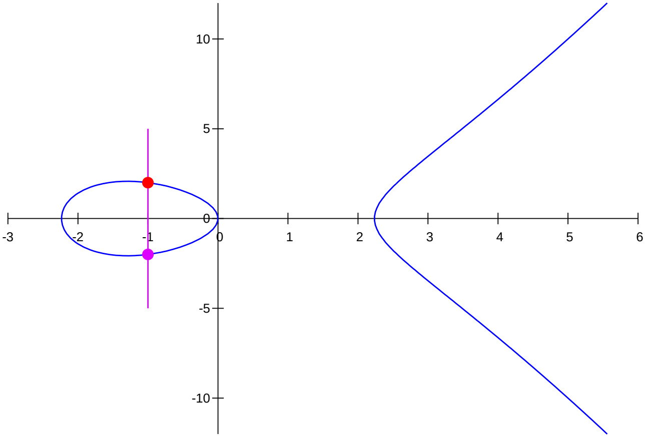
Also known as Chord & Tangent Addition Law.

Inverses on Elliptic Curves

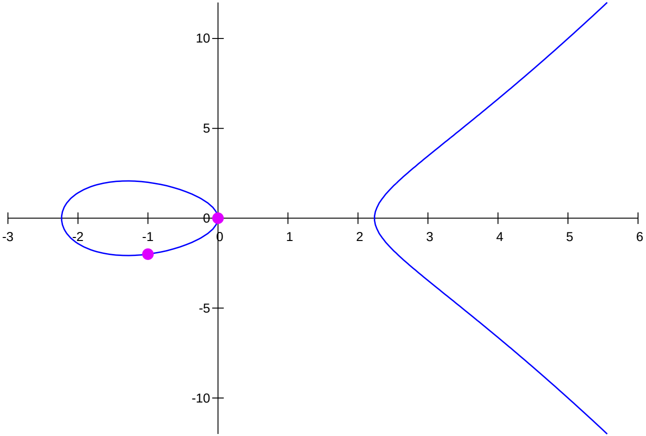


$-(\bullet) = ?$

Inverses on Elliptic Curves

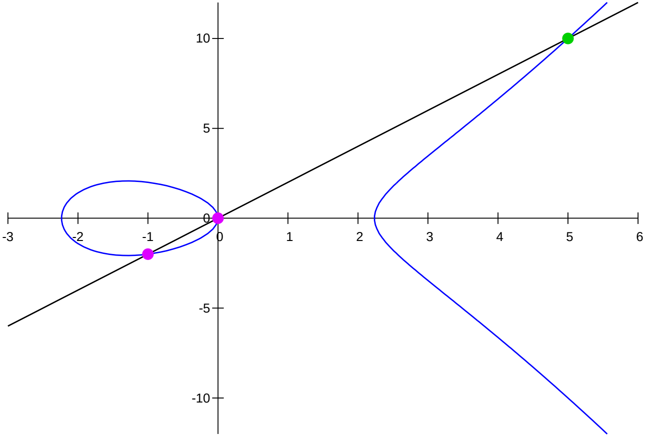


$$\textcolor{magenta}{\bullet} + \textcolor{red}{\bullet} + \infty = 0 \qquad \Rightarrow \qquad -(\textcolor{magenta}{\bullet}) = \textcolor{red}{\bullet}$$


10
5
0
-5
-10
-3
-2
-1
0
1
2
3
4
5
6

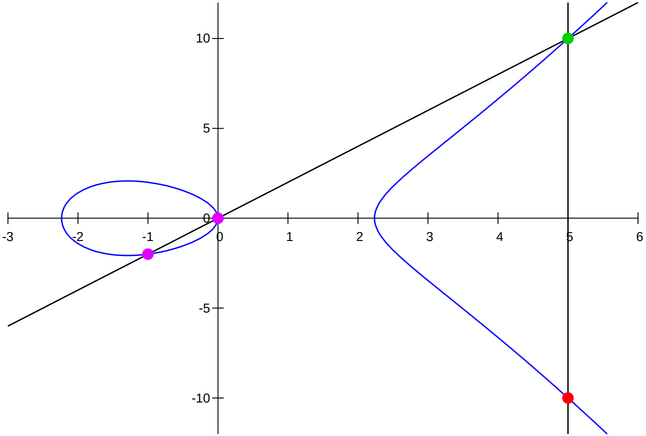
● + ● = ?

Addition on Elliptic Curves



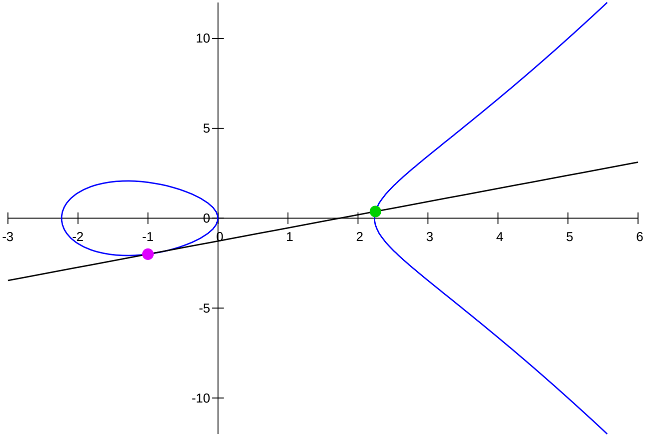
$\bullet + \bullet + \bullet = 0$

Addition on Elliptic Curves



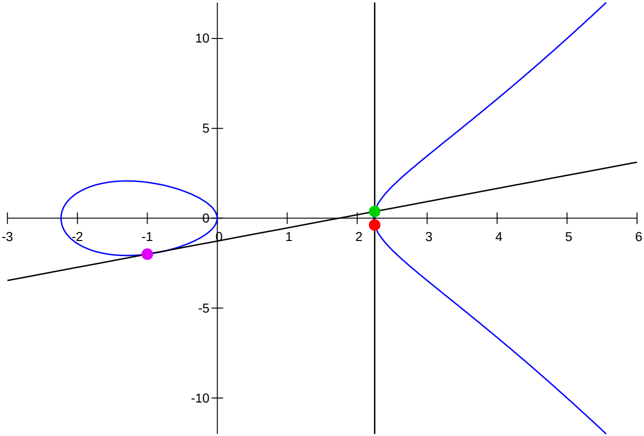
$$\bullet + \bullet + \bullet = 0 \quad \Rightarrow \quad \bullet + \bullet = \bullet$$

Doubling on Elliptic Curves



$2 \times \bullet = ?$

Doubling on Elliptic Curves



$2 \times$ ● $+$ ● $= 0 \qquad \Rightarrow \qquad 2 \times$ ● $=$ ●

Let

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \qquad (P_1 \neq \infty,\ P_2 \neq \infty,\ P_1 + P_2 \neq \infty)\ .$$

Then

$$\begin{aligned} -P_1 &= (-x_1, y_1) \\ P_1 + P_2 &= (\lambda^2 - x_1 - x_2,\ -\lambda^3 + \lambda(x_1 + x_2) - \mu) \end{aligned}$$

where

$$\boxed{\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \end{cases}} \qquad \boxed{\mu = \begin{cases} \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \dfrac{-x_1^3 + Ax_1 + 2B}{2y_1} & \text{if } P_1 = P_2 \end{cases}}$$

Recall Weierstraß equation:

$$E \ : \ y^2 + (\underbrace{a_1 x + a_3}_{h(x)})y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}$$

$\deg(f) = 3 = 2 \cdot 1 + 1$ odd

$\deg(h) = 1$ for $\mathrm{char}(K) = 2$; $h = 0$ for $\mathrm{char}(K) \neq 2$

Generalization: $\deg(f) = 2g + 1, \ \deg(h) \leq g$

g is the genus of the curve

$g = 1$: elliptic curves

$g = 2$: $\deg(f) = 5$, $\deg(h) \leq 2$ (always hyperelliptic).

Hyperelliptic Curves

Hyperelliptic curve of genus g **over** K:

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

- $h(x), f(x) \in K[x]$
- $f(x)$ monic and $\deg(f) = 2g + 1$ is odd
- $\deg(h) \leq g$ if $\mathrm{char}(K) = 2$; $h(x) = 0$ if $\mathrm{char}(K) \neq 2$
- non-singularity

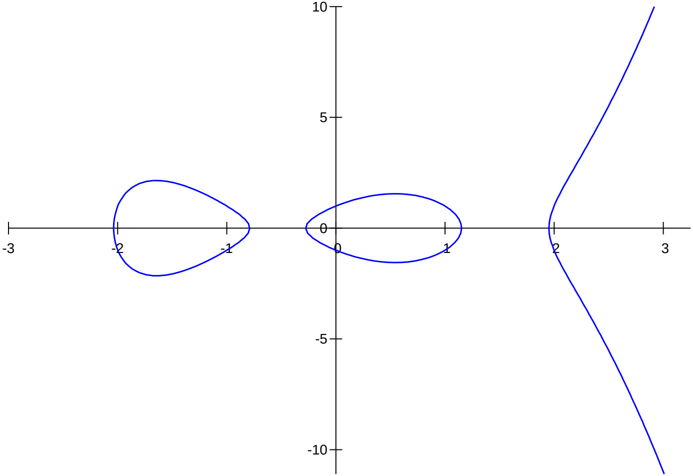
$\mathrm{char}(K) \neq 2$: $y^2 = f(x)$, $f(x)$ monic, of odd degree, square-free

Set of L-**rational** points on H $(K \subseteq L \subseteq \overline{K})$:

$$H(L) \ = \ \{(x_0, y_0) \in L \times L \mid y_0^2 + h(x_0)y = f(x_0)\} \cup \{\infty\}$$

An Example

$H : y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$, genus $g = 2$



Divisors

- Group of divisors on H:

$$\mathrm{Div}_H(\overline{K}) \;=\; \langle H(\overline{K})\rangle \;=\; \left\{ \sum_{\text{finite}} m_P P \mid m_P \in \mathbb{Z},\; P \in H(\overline{K}) \right\}$$

- Subgroup of $\mathrm{Div}_H(\overline{K})$ of degree zero divisors on H:

$$\mathrm{Div}^0_H(\overline{K}) \;=\; \langle [P] \mid P \in H(\overline{K})\rangle \;=\; \left\{ \sum_{\text{finite}} m_P [P] \mid m_P \in \mathbb{Z},\; P \in H(\overline{K}) \right\}$$

  where $[P] = P - \infty$

- Subgroup of $\mathrm{Div}^0_H(\overline{K})$ of principal divisors on H:

$$\mathrm{Prin}_H(\overline{K}) \;=\; \left\{ \sum_{\text{finite}} v_P(\alpha)[P] \mid \alpha \in K(x,y),\; P \in H(\overline{K}) \right\}$$

The Jacobian

Jacobian of H: $\mathrm{Jac}_H(\overline{K}) = \mathrm{Div}^0_H(\overline{K})/\mathrm{Prin}_H(\overline{K})$

Motto: "*Any complete collection of points on a function sums to zero.*"

$$H(\overline{K}) \hookrightarrow \mathrm{Jac}_H(\overline{K}) \quad \text{via} \quad P \mapsto [P]$$

For elliptic curves: $E(\overline{K}) \cong \mathrm{Jac}_E(\overline{K}) \quad (\Rightarrow \ E(\overline{K})$ is a group)

Identity: $[\infty] = \infty - \infty$

Inverses: The points

$$P = (x_0, y_0) \ \text{ and } \ \overline{P} = (x_0, -y_0 - h(x_0))$$

on H both lie on the function $x = x_0$, so

$$-[P] = [\overline{P}]$$

Semi-Reduced and Reduced Divisors

Every class in $\mathrm{Jac}_H(\overline{K})$ contains a divisor $\sum\limits_{\text{finite}} m_P[P]$ such that

- all $m_P > 0$ (replace $-[P]$ by $[\overline{P}]$)
- if $P = \overline{P}$, then $m_P = 1$ (as $2[P] = 0$)
- if $P \neq \overline{P}$, then only one of P, $\overline{P}$ can appear in the sum (as $[P] + [\overline{P}] = 0$)

Such a divisor is **semi-reduced**. If $\sum m_P \leq g$, then it is **reduced**.

E.g. $g = 2$: reduced divisors are of the form $[P]$ or $[P] + [Q]$.

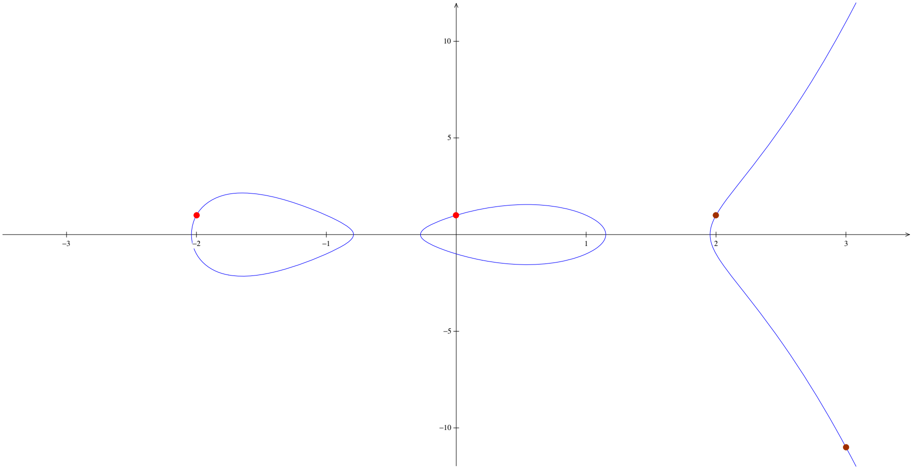
Theorem

Every class in $\mathrm{Jac}_H(\overline{K})$ contains a unique reduced divisor.

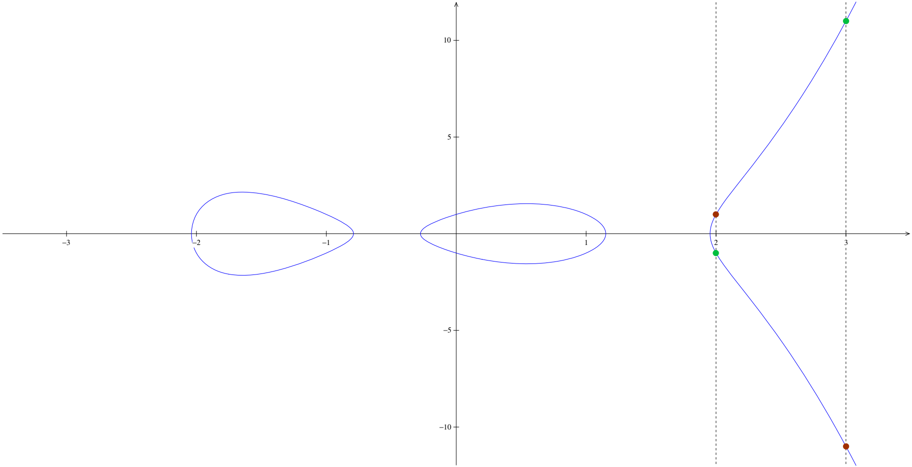
For reduced D_1, D_2, the reduced divisor in the class $[D_1 + D_2]$ is denoted $D_1 \oplus D_2$.

An Example of Reduced Divisors

$D_1 = (-2, 1) + (0, 1)$, $D_2 = (2, 1) + (3, -11)$

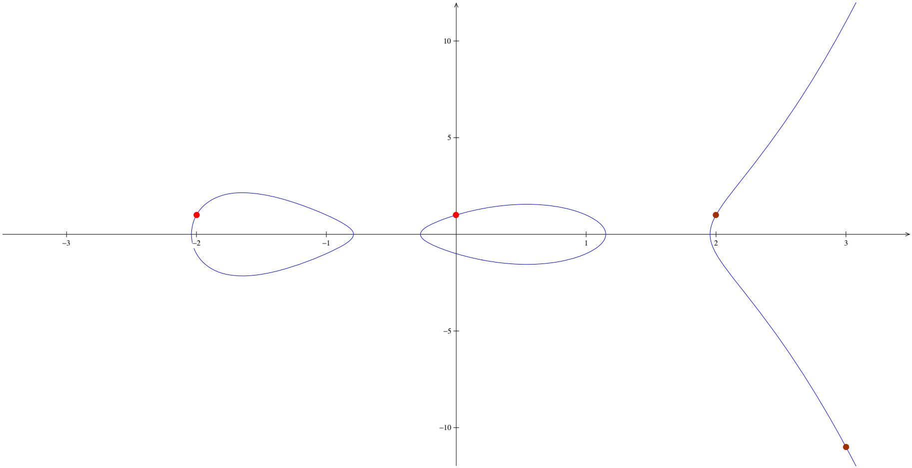


The inverse of $D = P_1 + P_2 + \cdots P_r$ is $-D = \overline{P}_1 + \overline{P}_2 + \cdots \overline{P}_r$

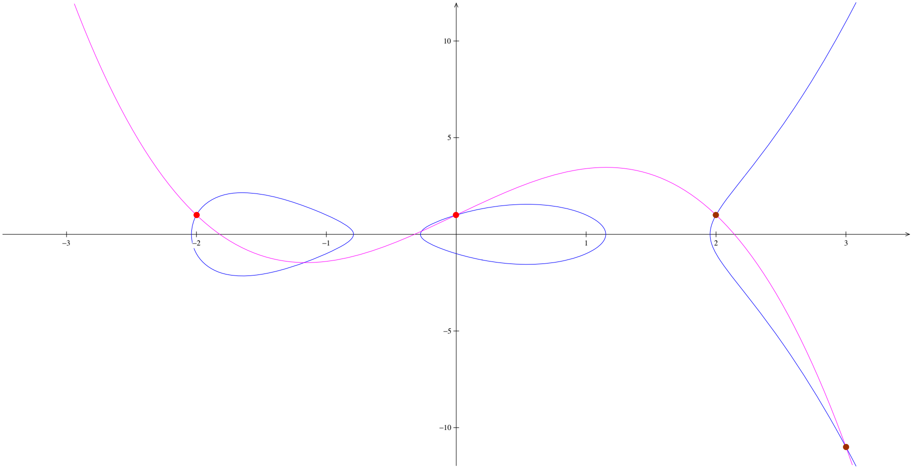


$-(\bullet + \bullet) = (\bullet + \bullet)$

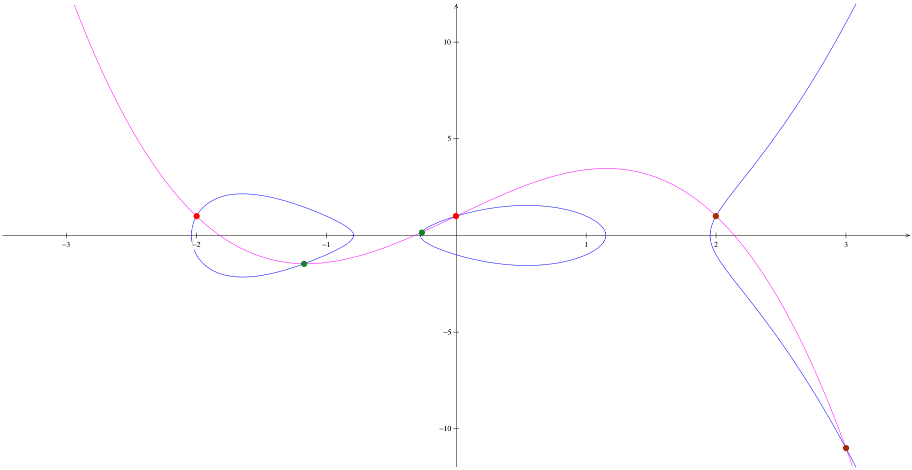
Addition on Genus 2 Curves



Addition on Genus 2 Curves

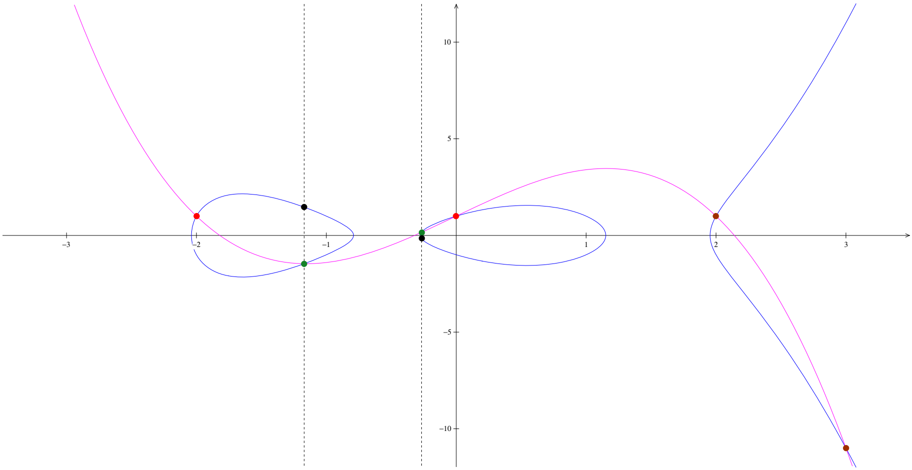


Addition on Genus 2 Curves



(● + ●) + (● + ●) + (● + ●) = 0

Addition on Genus 2 Curves



$(\bullet + \bullet) + (\bullet + \bullet) + (\bullet + \bullet) = 0 \quad \Rightarrow \quad (\bullet + \bullet) \oplus (\bullet + \bullet) = (\bullet + \bullet)$

Addition on Genus 2 Curves

UNIVERSITY OF CALGARY

Motto: "*Any complete collection of points on a function sums to zero.*"

To add and reduce two divisors $P_1 + P_2$ and $Q_1 + Q_2$ in genus 2:

- The four points P_1, P_2, Q_1, Q_2 lie on a unique function $y = v(x)$ with $\deg(v) = 3$.
- This function intersects H in two more points R_1 and R_2:
  - The x-coordinates of R_1 and R_2 can be obtained by finding the remaining two roots of $v(x)^2 + h(x)v(x) = f(x)$.
  - The y-coordinates of R_1 and R_2 can be obtained by substituting the x-coordinates into $y = v(x)$.
- Since $(P_1 + P_2) + (Q_1 + Q_2) + (R_1 + R_2) = 0$, we have

$$(P_1 + P_2) \oplus (Q_1 + Q_2) = \overline{R_1} + \overline{R_2} \ .$$

Consider $H : y^2 = f(x)$ with $f(x) = x^5 - 5x^3 + 4x + 1$ over $\mathbb{Q}$.

To add & reduce $(-2, 1) + (0, 1)$ and $(2, 1) + (3, -11)$, proceed as follows:

- The unique degree 3 function through $(-2, 1)$, $(0, 1)$, $(2, 1)$ and $(3, -11)$ is $y = v(x)$ with $v(x) = -(4/5)x^3 + (16/5)x + 1$.
- The equation $v(x)^2 = f(x)$ becomes

$$(x - (-2))(x - 0)(x - 2)(x - 3)(16x^2 + 23x + 5) = 0 \ .$$

- The roots of $16x^2 + 23x + 5$ are $\dfrac{-23 \pm \sqrt{209}}{32}$.
- The corresponding y-coordinates are $\dfrac{-1333 \pm 115\sqrt{209}}{2048}$. So

$(-2, 1) + (0, 1) \ \oplus \ (2, 1) + (3, -11) =$

$$\left(\frac{-23 + \sqrt{209}}{32}, \frac{1333 - 115\sqrt{209}}{2048}\right) + \left(\frac{-23 - \sqrt{209}}{32}, \frac{1333 + 115\sqrt{209}}{2048}\right).$$

Hyperelliptic Addition in General

Let D_1, D_2 be reduced divisors on $H : y^2 + h(x)y = f(x)$.

First form the **semi-reduced sum** of D_1 and D_2, obtaining $D = \sum_{i=1}^{r} [P_i]$

Now iterate over D as follows, until $r \le g$:

- The r points P_i all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$.
- $w(x) = v^2 - hv - f$ is a polynomial of degree $\max\{2r-2, 2g+1\}$. r of the roots of $w(x)$ are the x-coordinates of the P_i.
- If $r \ge g + 2$, then $\deg(w) = 2r - 2$, yielding $r - 2$ further roots. If $r = g + 1$, then $\deg(w) = 2g + 1$, yielding g further roots.
- Substitute these new roots into $y = v(x)$ to obtain $\max\{r-2, g\}$ new points on H. Replace D by the new divisor thus obtained.

Since $r \le 2g$ at the start, $D_1 \oplus D_2$ is obtained after at most $\lceil g/2 \rceil$ steps.

Mumford Representation

Let $D = \sum_{i=1}^{r} m_i[P_i]$ be a semi-reduced divisor, $P_i = (x_i, y_i)$

The **Mumford representation** of D is a pair of polynomials $(u(x), v(x))$ that uniquely determines D:

$u(x)$ captures all the x-coordinates with multiplicities;

$y = v(x)$ is the interpolation function through all the P_i (as before).

Formally:

$$u(x) = \prod_{i=1}^{r} (x - x_i)^{m_i}$$

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 + v(x)h(x) - f(x)\right]_{x=x_i} = 0 \qquad (0 \le j \le m_i - 1)$$

Properties and Examples

Properties:

- $u(x_i) = 0$ and $v(x_i) = y_i$ with multiplicity m_i for $1 \leq i \leq r$;
- $u(x)$ is monic and divides $v(x)^2 + h(x)v(x) - f(x)$
- D uniquely determines $u(x)$ and $v(x)$ mod $u(x)$;
- Any pair of polynomials $u(x)$, $v(x) \in \overline{K}[x]$ with $u(x)$ monic and dividing $v(x)^2 + h(x)v(x) - f(x)$ determines a semi-reduced divisor.

Examples:

- If $D = [(x_0, y_0)]$ is a point, then $u(x) = x - x_0$ and $v(x) = y_0$.
- If $D = [(x_1, y_1)] \oplus [(x_2, y_2)]$, then

  $u(x) = (x - x_1)(x - x_2)$,

  $y = v(x)$ is the line through (x_1, y_1) and (x_2, y_2).

UNIVERSITY OF CALGARY

Let $D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$.

Simplest case: for any $[P]$ occurring in D_1, $[\overline{P}]$ doesn't occur in D_2 and vice versa. Then $D_1 + D_2 = (u, v)$ is semi-reduced and

$$u = u_1 u_2 \ , \quad v = \begin{cases} v_1 \pmod{u_1} \ , \\ v_2 \pmod{u_2} \ . \end{cases}$$

In general: suppose $P = (x_0, y_0)$ occurs in D_1 and $\overline{P}$ occurs in D_2.

Then $u_1(x_0) = u_2(x_0) = 0$ and $v_1(x_0) = y_0 = -v_2(x_0) - h(x_0)$, so $x - x_0$ divides $u_1(x)$, $u_2(x)$, $v_1(x) + v_2(x) + h(x)$.

$$d = \gcd(u_1, u_2, v_1 + v_2 + h) = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2 + h).$$

$$u = u_1 u_2 / d^2.$$

$$v \equiv \frac{1}{d}\left(s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)\right) \pmod{u}$$

(In the simplest case above, $d = 1$ and $s_3 = 0$)

Reduction Via Mumford Reps

Let $D = (u, v)$ be a semi-reduced divisor on $H : y^2 + h(x)y = f(x)$.

While $\deg(u) > g$ do

// Replace the x-coordinates of the points in D by those of the other intersection points of H with v:

$$u \leftarrow (f - vh - v^2)/u \quad .$$

// Replace the new points by their opposites:

$$v \leftarrow (-v - h) \pmod{u} \quad .$$

Mumford Arithmetic — Example

Consider again $H : y^2 = f(x)$ with $f(x) = x^5 - 5x^3 + 4x + 1$ over $\mathbb{Q}$.

Compute $D_1 \oplus D_2$ with $D_1 = (-2, 1) + (0, 1)$ and $D_2 = (2, 1) + (3, -11)$:

Mumford rep of D_1: $u_1(x) = x^2 + 2x$, $v_1(x) = 1$.

Mumford rep of D_2: $u_2(x) = x^2 - 5x + 6$, $v_2(x) = -12x + 25$.

$$u(x) = u_1(x)u_2(x) = x^4 - 3x^3 - 4x^2 + 12x \ ;$$

$$v(x) = -(4/5)x^3 + (16/5)x + 1 \ ;$$

$$u(x) \leftarrow (f(x) - v(x)^2)/u(x) = 16x^2 + 23x + 5 \ ;$$

$$v \leftarrow -v \pmod{u} = (16x - 23)/320 \ ;$$

Mumford rep of $D_1 \oplus D_2 = \left(\frac{-23+\sqrt{209}}{32}, \frac{1333-115\sqrt{209}}{2048}\right) + \left(\frac{-23-\sqrt{209}}{32}, \frac{1333+115\sqrt{209}}{2048}\right)$:

$$u(x) = 16x^2 + 23x + 5, \ v(x) = (16x - 23)/320.$$

Divisors defined over K

Let $\phi \in \mathrm{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$).

ϕ acts on points via their coordinates, and on divisors via their points.

A divisor D is **defined over** K if $\phi(D) = D$ for all $\phi \in \mathrm{Gal}(\overline{K}/K)$.

Example: The divisor

$$D = \left(\frac{-23+\sqrt{209}}{32}, \frac{1333-115\sqrt{209}}{2048} \right) + \left(\frac{-23-\sqrt{209}}{32}, \frac{1333+115\sqrt{209}}{2048} \right)$$

is defined over $\mathbb{Q}$ (invariant under automorphism $\sqrt{209} \mapsto -\sqrt{209}$).

Theorem

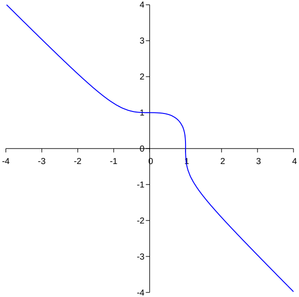
$D = (u, v)$ is defined over K if and only if $u(x), v(x) \in K[x]$.

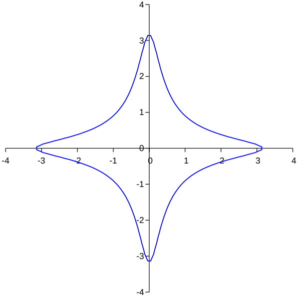
Corollary

If K is a finite field, then $\mathrm{Jac}(H)$ is finite.

Some Other Elliptic Curve Models

- **Hessians**: $x^3 + y^3 - 3dxy = 1$
- **Edwards models**: $x^2 + y^2 = c^2(1 + dx^2y^2)$ (q odd) and variations

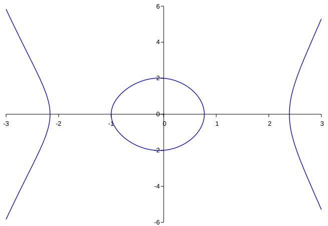




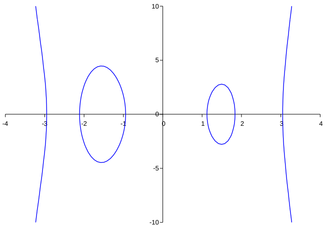
$x^3 + y^3 = 1$

$x^2 + y^2 = 10(1 - x^2y^2)$

$y^2 + h(x)y = f(x)$, $\deg(f) = 2g + 2$, $\deg(h) = g + 1$ if $\mathrm{char}(K) = 2$.



$$y^2 = x^4 - 6x^2 + x + 6$$
$$(g = 1)$$



$$y^2 = x^6 - 13x^4 + 44x^2 - 4x - 1$$
$$(g = 2)$$

Properties of Even Degree Models

UNIVERSITY OF CALGARY

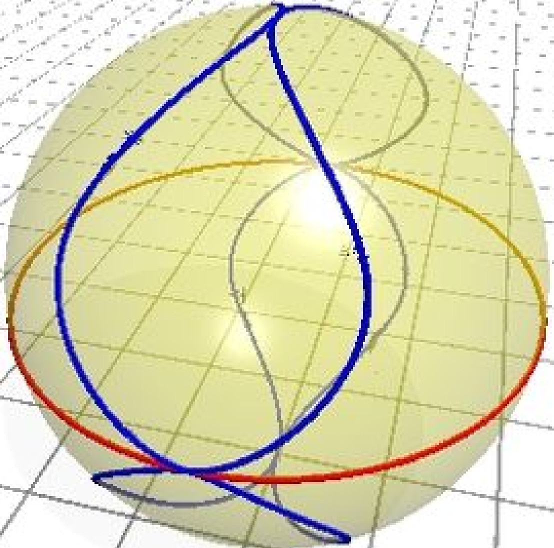
- More general and plentiful than odd degree hyperelliptic curves:
  - can always transform an odd to even degree model over K, but the reverse direction may require an extension of K.
- Two points at infinity (∞ and $\overline{\infty}$).
- Divisor Representation: $\sum_{i=1}^{r} P_i - r\infty + n(\overline{\infty} - \infty), \quad r \leq g.$
  - No restrictions on n: many reduced divisors in each class ($\approx q^g$)
  - $n = 0$: infrastructures (misses a few divisor classes)
  - $n \approx g$: unique representatives (Paulus-Rück 1999)
  - $n \approx \lceil g/2 \rceil$: balanced representation, unique and much better for computation (Galbraith-Harrison-Mireles Morales 2008)
- The DLP's in all these settings are polynomially equivalent.

Conclusion and Work in Progress

UNIVERSITY OF CALGARY

- Genus 1 and 2, q prime or $q = 2^n$: efficient and secure for DLP based crypto. Genus 3 might also be OK.
- Explicit formulas reduce the polynomial arithmetic to arithmetic in $\mathbb{F}_q$.
  Odd degree: LOTS of literature on genus 2, a bit on genus 3 and 4;
  Even degree: reasonably developed for genus 2, work on genus 3 in progress.
- Other coordinates (e.g. projective coordinates) can be more efficient. They avoid inversions in $\mathbb{F}_q$, at the expense of redundancy. Oftentimes *mixed* coordinates are best.
- For genus 1, use Edwards models — more efficient, *unified* formulas. No higher genus Edwards analogue is known.
- For genus 2 and odd degree, Gaudry's *Kummer surface* arithmetic is fastest, but doesn't work for all curves.
- Work on arbitrary genus is ongoing.

Thank you! Questions?



$y^2 = x^6 + x^2 + x$

http://voltage.typepad.com/superconductor/2011/09/a-projective-imaginary-hyperelliptic-curve.html