An Introduction to Hyperelliptic Curves

David Gruenewald

davidg@maths.usyd.edu.au

eRISCS, Université de la Méditerranée

4th June 2009

Definitions

A hyperelliptic curve H over a field K is defined by

$$y^2 + h(x)y = f(x)\,, \quad h, f \in K[x]$$

with $\deg(h) \leq g$ and $\deg(f) = 2g + 1$.

- When $\mathrm{char}(K) \neq 2$, we can take $h(x) = 0$.
- The integer $g \geq 0$ is called the genus of the curve.
- $g = 1 \Longrightarrow$ elliptic curves.

Definitions

A hyperelliptic curve H over a field K is defined by

$$y^2 + h(x)y = f(x)\,, \quad h, f \in K[x]$$

with $\deg(h) \leq g$ and $\deg(f) = 2g + 1$.

- When $\mathrm{char}(K) \neq 2$, we can take $h(x) = 0$.
- The integer $g \geq 0$ is called the genus of the curve.
- $g = 1 \Longrightarrow$ elliptic curves.

The set of K-rational points is

$$H(K) := \{(x, y) \in K \times K \mid y^2 + h(x)y = f(x)\} \cup \{\infty\}$$

Question: Is $H(K)$ a group? No, but...

Hyperelliptic Jacobians

For $g \geq 1$ there exists a smallest abelian group $J_H(K)$ in which $H(K)$ embeds, called the Jacobian of H.

$$\begin{array}{rccc} [\cdot]: & H(K) & \hookrightarrow & J_H(K) \\ & \infty & \longmapsto & [\infty] = 0 \end{array}$$

Hyperelliptic Jacobians

For $g \geq 1$ there exists a smallest abelian group $J_H(K)$ in which $H(K)$ embeds, called the Jacobian of H.

$$\begin{array}{rccc} [\cdot]: & H(K) & \hookrightarrow & J_H(K) \\ & \infty & \longmapsto & [\infty] = 0 \end{array}$$

Explicitly

$$J_H(\overline{K}) = \mathrm{Div}_{\overline{K}}(H)/\mathrm{Int}_{\overline{K}}(H)$$

where

$$\mathrm{Div}_{\overline{K}}(H) := \left\{ \sum_{\text{finite}} m_i[P_i] \ : \ m_i \in \mathbb{Z}, \ P_i \in H(\overline{K}) \right\}$$

and

$$\mathrm{Int}_{\overline{K}}(H) := \left\langle \sum \mathrm{ord}_P(g)[P] \ : \ 0 \neq g \in K[H] \right\rangle$$

is the subgroup generated by interesction divisors $H \cap \{g(x,y)=0\}$

Example (opposite points)

Let $P = (x_0, y_0) \in H$; write $\widetilde{P} = (x_0, -y_0 - h(x_0))$.
Since $H \cap \{x = x_0\} = [P] + [\widetilde{P}] \in \mathrm{Int}(H)$ we have $[\widetilde{P}] = -[P]$.

$\Longrightarrow$ by replacing P_i with $\widetilde{P}_i$ in $\sum m_i[P_i]$ we can assume that $m_i > 0$ for all i.

Example (opposite points)

Let $P = (x_0, y_0) \in H$; write $\widetilde{P} = (x_0, -y_0 - h(x_0))$.
Since $H \cap \{x = x_0\} = [P] + [\widetilde{P}] \in \mathrm{Int}(H)$ we have $[\widetilde{P}] = -[P]$.

$\Longrightarrow$ by replacing P_i with $\widetilde{P}_i$ in $\sum m_i[P_i]$ we can assume that $m_i > 0$ for all i.

Every nonzero element of $J_H(\overline{K})$ can be written as $D = \sum m_i[P_i]$ such that

- $m_i > 0$;
- $m_i = 1$ if $P_i = \widetilde{P}_i$ (becuase $2[P_i] = 0$);
- if $P \neq \widetilde{P}$ then only one of $\{P, \widetilde{P}\}$ can appear in the sum.

A divisor written in this form is said to be semi-reduced.

Example (opposite points)

Let $P = (x_0, y_0) \in H$; write $\widetilde{P} = (x_0, -y_0 - h(x_0))$.
Since $H \cap \{x = x_0\} = [P] + [\widetilde{P}] \in \mathrm{Int}(H)$ we have $[\widetilde{P}] = -[P]$.

$\Longrightarrow$ by replacing P_i with $\widetilde{P}_i$ in $\sum m_i[P_i]$ we can assume that $m_i > 0$ for all i.

Every nonzero element of $J_H(\overline{K})$ can be written as $D = \sum m_i[P_i]$ such that

- $m_i > 0$;
- $m_i = 1$ if $P_i = \widetilde{P}_i$ (becuase $2[P_i] = 0$);
- if $P \neq \widetilde{P}$ then only one of $\{P, \widetilde{P}\}$ can appear in the sum.

A divisor written in this form is said to be semi-reduced.
If $\deg(D) := \sum m_i \leq g$ we say that D is reduced.

Theorem (Cantor's algorithm)

Every element of $J_H(\overline{K})$ is equivalent to a unique reduced divisor.

A semi-reduced divisor $D = \sum m_i[P_i]$ can be compactly written using Mumford representation: $\langle u(x), v(x) \rangle$ where

- $u(x) = \prod (x - x_i)^{m_i}$
- $\deg(v) < \deg(u)$ is the unique polynomial which satisfies

$$v(x_i) = y_i \quad \text{and} \quad u | (v^2 + vh - f).$$

Eg. $[(x_0, y_0)] \in J_H(K)$ has Mumford representation $\langle x - x_0, y_0 \rangle$.

A semi-reduced divisor $D = \sum m_i[P_i]$ can be compactly written using Mumford representation: $\langle u(x), v(x) \rangle$ where

- $u(x) = \prod (x - x_i)^{m_i}$
- $\deg(v) < \deg(u)$ is the unique polynomial which satisfies

$$v(x_i) = y_i \quad \text{and} \quad u | (v^2 + vh - f).$$

Eg. $[(x_0, y_0)] \in J_H(K)$ has Mumford representation $\langle x - x_0, y_0 \rangle$.

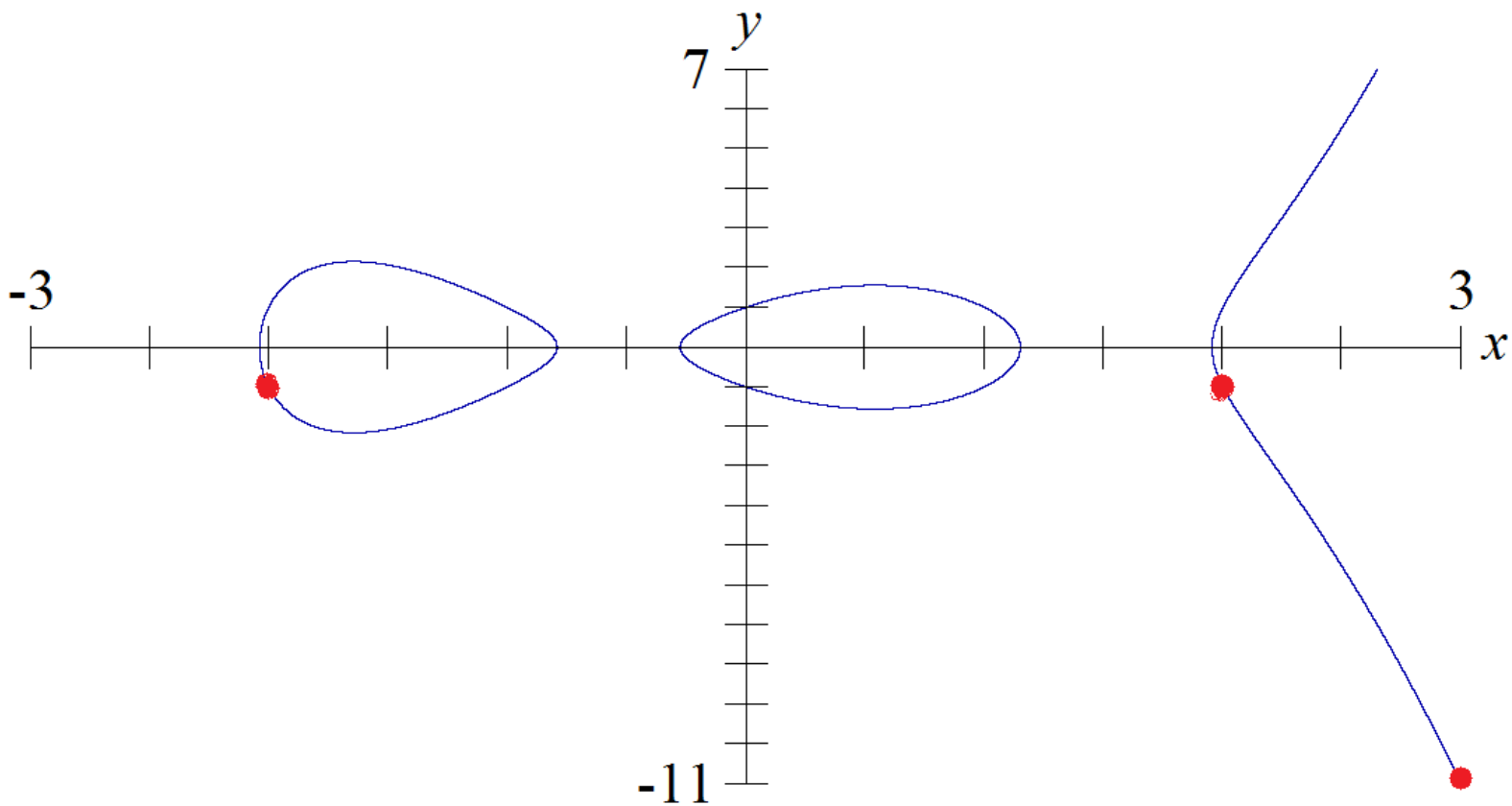
Defn : A reduced divisor $D = \langle u(x), v(x) \rangle \in J_H(\overline{K})$ is K-rational if $u, v \in K[x]$. These form the points of $J_H(K)$.

The sum of two (semi-) reduced divisors $D_1, D_2 \in J_H(K)$ can be computed efficiently using Cantor's algorithm:

1. Composition: form a semi-reduced divisor D' representing the sum $D_1 + D_2$.
2. Reduction: transform D' into a reduced divisor.

Example curve $H: \ y^2 = x(x^2-1)(x^2-4)+1$

Red points: $R_1 = (-2,-1), \ R_2 = (2,-1), \ R_3 = (3,-11)$
Semireduced divisor for $[R_1]+[R_2]+[R_3]$ is
$\langle (x-3)(x-2)(x+2), \ -2x^2+7 \rangle$.



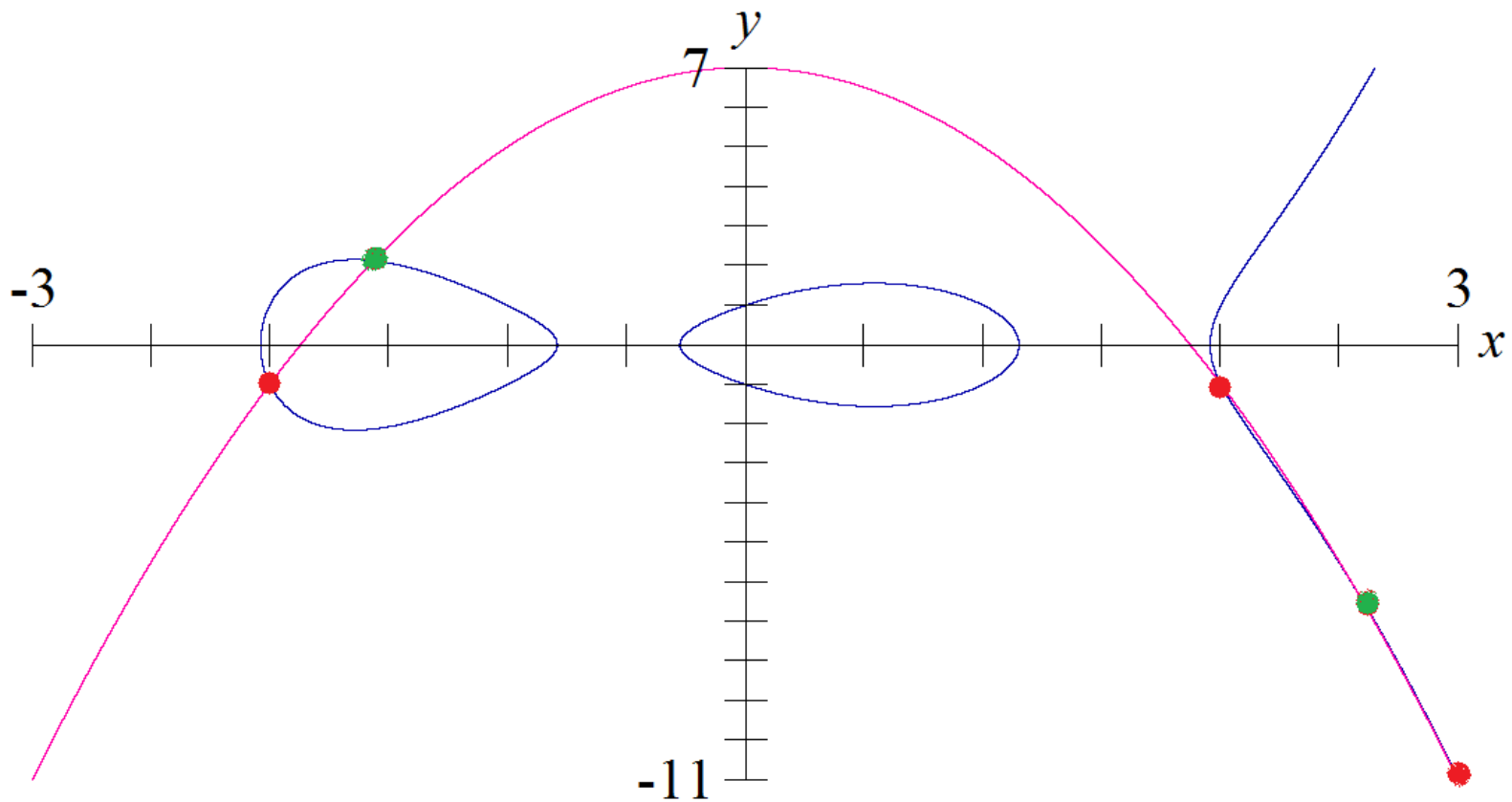
Example curve $H: \ y^2 = x(x^2-1)(x^2-4)+1$

Red points: $R_1 = (-2,-1), \ R_2 = (2,-1), \ R_3 = (3,-11)$

Semireduced divisor for $[R_1]+[R_2]+[R_3]$ is

$\langle (x-3)(x-2)(x+2), \ -2x^2+7 \rangle$.

$H \cap \{y = -2x^2+7\} = [R_1]+[R_2]+[R_3]+[G_1]+[G_2] = 0 \in J_H(\mathbb{Q})$



Example curve $H: \ y^2 = x(x^2-1)(x^2-4)+1$

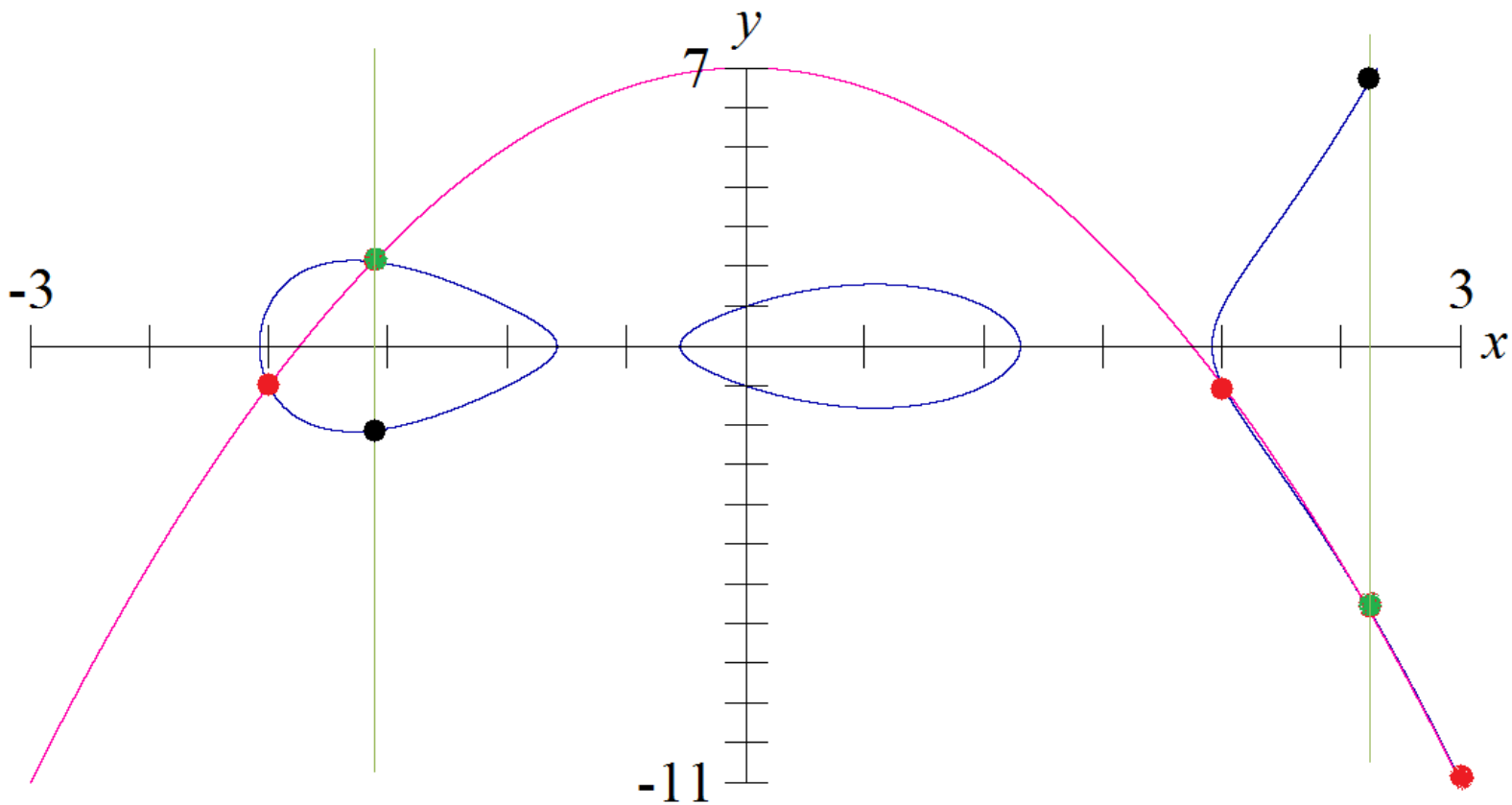
Red points: $R_1 = (-2,-1), \ R_2 = (2,-1), \ R_3 = (3,-11)$

Semireduced divisor for $[R_1]+[R_2]+[R_3]$ is

$\langle (x-3)(x-2)(x+2), \ -2x^2+7 \rangle$.

$H \cap \{y = -2x^2+7\} = [R_1]+[R_2]+[R_3]+[G_1]+[G_2] = 0 \in J_H(\mathbb{Q})$

$\Rightarrow [R_1]+[R_2]+[R_3] = -[G_1]-[G_2] = [B_1]+[B_2]$.



Example curve $H: \ y^2 = x(x^2-1)(x^2-4)+1$

Red points: $R_1 = (-2,-1), \ R_2 = (2,-1), \ R_3 = (3,-11)$
Semireduced divisor for $[R_1]+[R_2]+[R_3]$ is
$\langle (x-3)(x-2)(x+2), \ -2x^2+7 \rangle$.
$H \cap \{y = -2x^2+7\} = [R_1]+[R_2]+[R_3]+[G_1]+[G_2] = 0 \in J_H(\mathbb{Q})$
$\Rightarrow [R_1]+[R_2]+[R_3] = -[G_1]-[G_2] = [B_1]+[B_2]$.

Cantor's algorithm outputs the divisor $\langle x^2-x-4, \ 2x+1 \rangle$ so the divisor is

$$[(2+\sqrt{5}, 16+7\sqrt{5})]+[(2-\sqrt{5}, 16-7\sqrt{5})]$$

which a $\mathbb{Q}$-rational point!
(the isomorphism

$$\sqrt{5} \mapsto -\sqrt{5}$$

switches the points but preserves the sum).

A nice fact

$$\boxed{J_H(\mathbb{F}_q) \approx q^g}$$

$\Longrightarrow$ We can form large groups relative to the key size.

Example

$H: \ y^2 + xy = x^{21} + 1$ over $\mathbb{F}_{2^d}$ (genus 10)

d	$\#J_H(\mathbb{F}_{2^d})$
1	$2^4 \cdot 211$

A nice fact

$$\boxed{J_H(\mathbb{F}_q) \approx q^g}$$

$\Longrightarrow$ We can form large groups relative to the key size.

Example

$H: \ y^2 + xy = x^{21} + 1$ over $\mathbb{F}_{2^d}$ (genus 10)

d	$\#J_H(\mathbb{F}_{2^d})$
1	$2^4 \cdot 211$
17	$2^4 \cdot 211 \cdot 2121156199 \cdot 252507580361 \cdot 284601993547 \cdot 2925604780864223$
19	$2^4 \cdot 211 \cdot 459905328497188154889884058354414661810212556369210033$
23	$2^4 \cdot 211 \cdot 1289 \cdot 737177344105848507047704 7 \cdot 5370172597172987672353340036488640083$

A nice fact

$$\boxed{J_H(\mathbb{F}_q) \approx q^g}$$

$\Longrightarrow$ We can form large groups relative to the key size.

Example

$H: \ y^2 + xy = x^{21} + 1$ over $\mathbb{F}_{2^d}$ (genus 10)

d	$\#J_H(\mathbb{F}_{2^d})$
1	$2^4 \cdot 211$
17	$2^4 \cdot 211 \cdot 2121156199 \cdot 252507580361 \cdot 284601993547 \cdot 2925604780864223$
19	$2^4 \cdot 211 \cdot 459905328497188154889884058354414661810212556369210033$
23	$2^4 \cdot 211 \cdot 1289 \cdot 737177344105848850704770 47 \cdot 5370172597172987672353340036488640083$

So we obtain a cyclic group in $J_H(\mathbb{F}_{2^{19}})$ of size $\approx 2^{178}$!!

A nice fact

$$\boxed{J_H(\mathbb{F}_q) \approx q^g}$$

$\Longrightarrow$ We can form large groups relative to the key size.

Example

$H: \ y^2 + xy = x^{21} + 1$ over $\mathbb{F}_{2^d}$ (genus 10)

d	$\#J_H(\mathbb{F}_{2^d})$
1	$2^4 \cdot 211$
17	$2^4 \cdot 211 \cdot 2121156199 \cdot 252507580361 \cdot 284601993547 \cdot 2925604780864223$
19	$2^4 \cdot 211 \cdot 459905328497188154889884058354414661810212556369210033$
23	$2^4 \cdot 211 \cdot 1289 \cdot 737177344105848850704770 47 \cdot 537017259717298767235340036488640083$

So we obtain a cyclic group in $J_H(\mathbb{F}_{2^{19}})$ of size $\approx 2^{178}$!!

But let's not get too excited..

Attacks on hyperelliptic Jacobians

The best algorithm for solving DLP in a generic abelian group G is Pollard's rho method which requires $O(\sqrt{\#G})$ group operations, that is, exponential in $\log \#G$.

$\Rightarrow$ DLP in $J_H(\mathbb{F}_q)$ can be solved in $O(q^{g/2})$ group operations.

Attacks on hyperelliptic Jacobians

The best algorithm for solving DLP in a generic abelian group G is Pollard's rho method which requires $O(\sqrt{\#G})$ group operations, that is, exponential in $\log \#G$.

$\Rightarrow$ DLP in $J_H(\mathbb{F}_q)$ can be solved in $O(q^{g/2})$ group operations.

When $g \geq 3$, index calculus algorithms for $J_H(\mathbb{F}_q)$ are effective:

- For $g \gtrsim \log_g(q)$ the algorithm is subexponential.
- For $3 \leq g \lesssim \log_g(q)$: not subexponential, but significantly better than Pollard's rho method: $\widetilde{O}(q^{2-2/g}) < O(q^{g/2})$.

This leaves us with genus 1 and 2.

Parameter choices

The majority of attacks on hyperelliptic curves are straightforward generalisations of attacks on elliptic curves:

- Pohlig-Hellman: reduces DLP on $J_H(\mathbb{F}_q)$ to subgroups of prime order. $\Rightarrow J_H(\mathbb{F}_q)$ must have a large prime factor r.
- Additive reduction: If $r|q$ then one can map DLP across to $(\mathbb{F}_r, +)$.
- Multiplicative reduction: can map DLP across to $(\mathbb{F}_{q^k}^{\times}, \times)$ where k is the smallest integer with $q^k \equiv 1 \pmod{r}$
  $\Rightarrow$ ensure k is large.
- Weil descent: In certain situations, $J_H(\mathbb{F}_{q^e}) \hookrightarrow J_X(\mathbb{F}_q)$ where X has larger genus and index calculus methods are quicker.
  $\Rightarrow$ ensure either q is prime, or $q = 2^f$ with f prime.

Making genus 2 competitive with elliptic curves

- arithmetic on the curve
- point counting
- isogenies
- CM method (endomorphism ring calculations)

Current research

algorithm	elliptic	hyperelliptic (genus 2)
arithmetic	Edwards curves	Kummer surfaces
point counting	SEA - $O(\log^{4+\varepsilon} q)$	$\exists$ polynomial time algorithm but it's impractical
explicit isogenies scalar mult: GLV:	Vélu's formulas: N-isogenies Frobenius	small degrees only: (ℓ, ℓ)-isogenies for $\ell = 2, 3$ Frobenius $\sqrt{D}$-multiplication
CM-method	Hilbert class polynomials	Igusa class polynomials

Current research

algorithm	elliptic	hyperelliptic (genus 2)
arithmetic	Edwards curves	Kummer surfaces
point counting	SEA - $O(\log^{4+\varepsilon} q)$	$\exists$ polynomial time algorithm but it's impractical
explicit isogenies scalar mult: GLV:	Vélu's formulas: N-isogenies Frobenius	small degrees only: (ℓ, ℓ)-isogenies for $\ell = 2, 3$ Frobenius $\sqrt{D}$-multiplication
CM-method	Hilbert class polynomials	Igusa class polynomials

Merci!