Hyperelliptic Curves, Cryptography and Factorization Algorithms

David Gruenewald

davidg@maths.usyd.edu.au

Radboud Universiteit Nijmegen

Algemeen Wiskundecolloquium
8th December 2010

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 $P_i = \widetilde{P}_i$ (because $2[P_i] = 0$);
- 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 $P_i = \widetilde{P}_i$ (because $2[P_i] = 0$);
- 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 $\langle x - x_0, y_0 \rangle$.

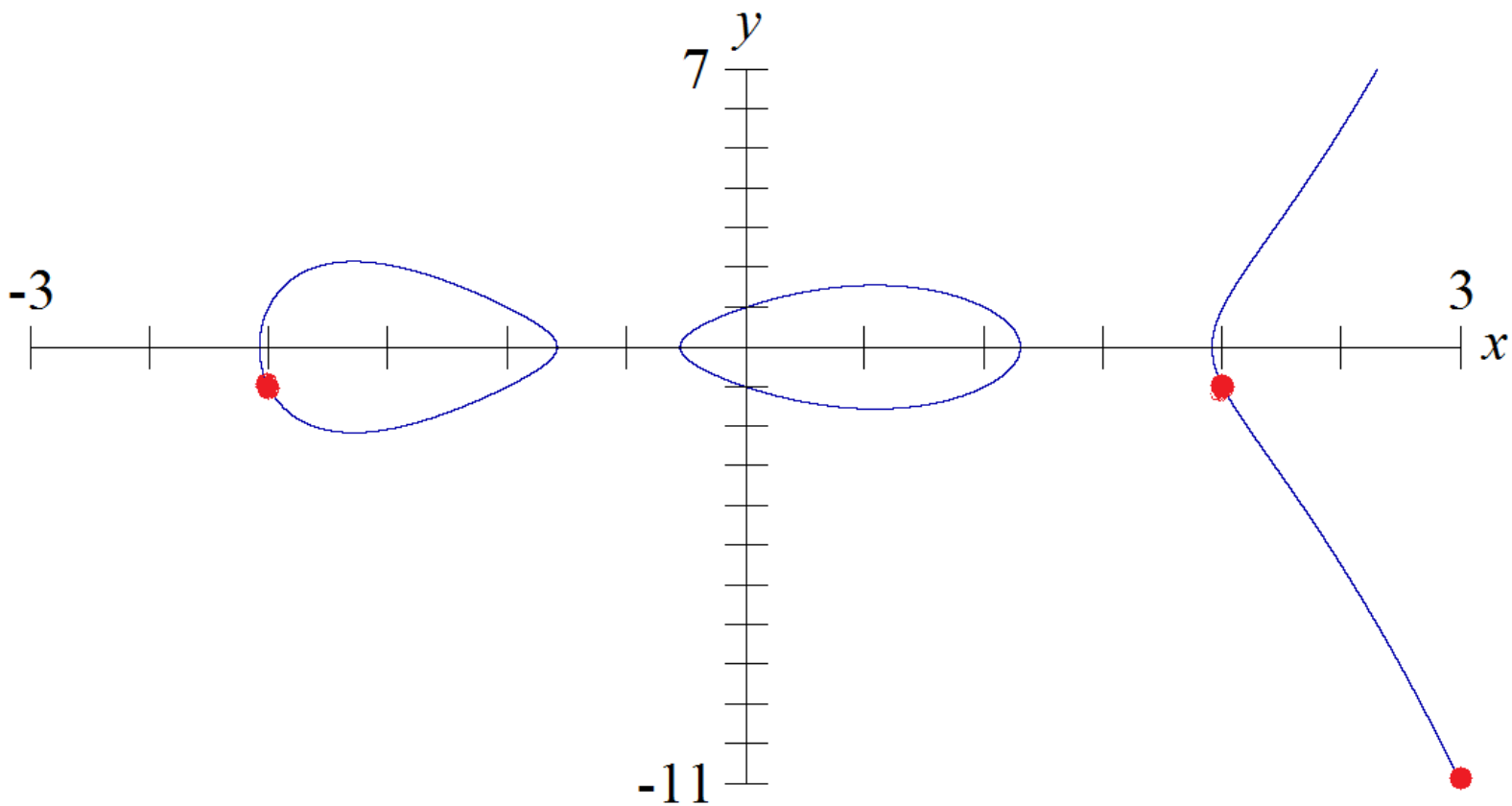
Defn : A reduced divisor $D = \langle u(x), v(x) \rangle \in J_H(\overline{K})$ is K-rational if $u, v \in K[x]$. These form the points of $J_H(K)$.

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



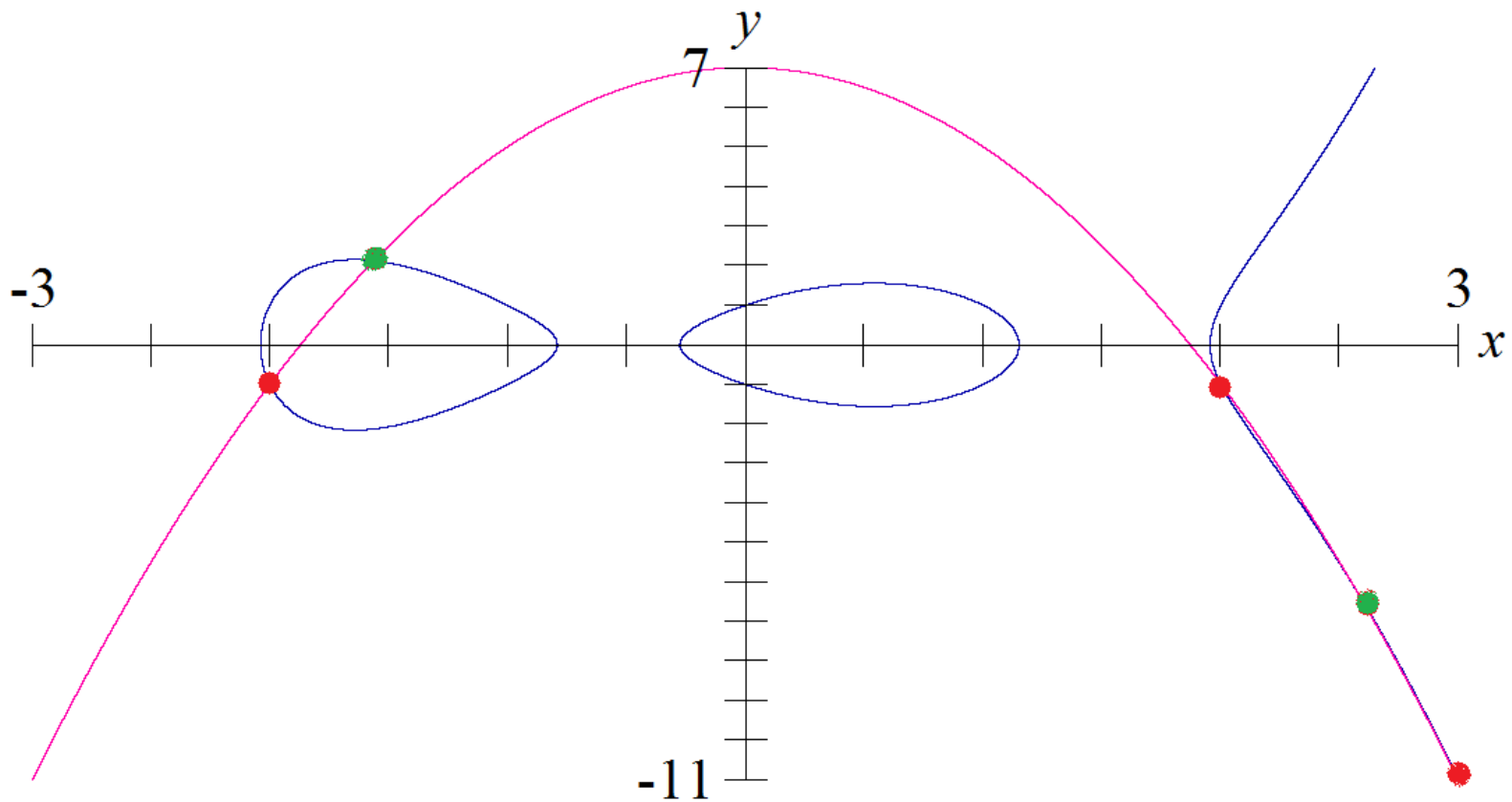
Example curve $H: \ y^2 = x(x^2-1)(x^2-4)+1$

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

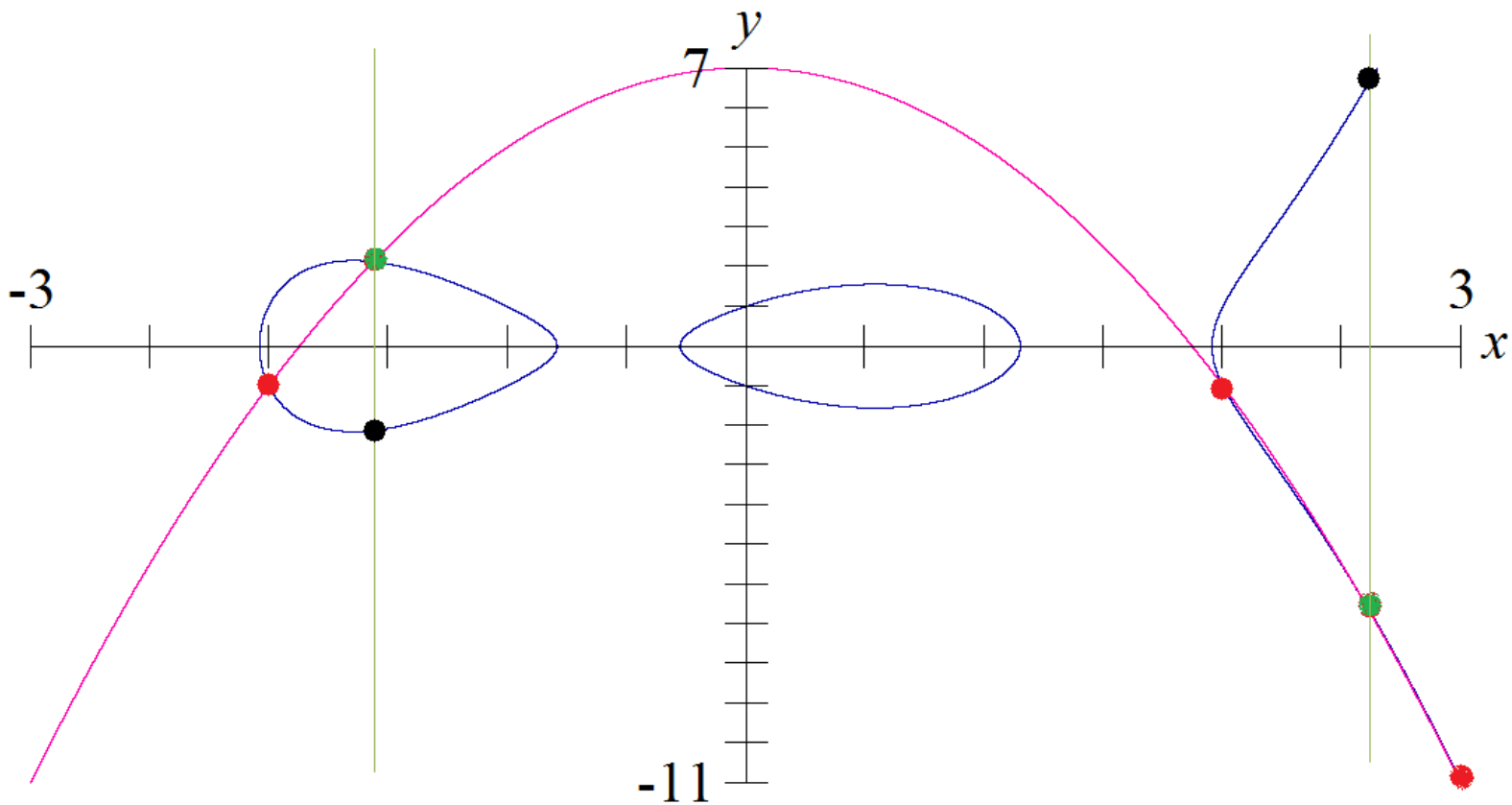
Red points: $R_1 = (-2,-1), \ R_2 = (2,-1), \ R_3 = (3,-11)$

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).

Composition steps

- Compute $d = \gcd(u_1, u_2, v_1 + v_2 + h)$ and s_i such that $d = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2 + h)$.
- Set $u_3 := u_1 u_2 / d^2$

$$v_3 := \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \pmod{u_3}$$

Reduction steps

- **while** $\deg(u_3) > g$ **do:**

  $u_3 := (f - v_3 h - v_3^2)/u_3$

  $v_3 := -h - v_3 \pmod{u_3}$

  end while
- Make u_3 monic
- return $\langle u_3, v_3 \rangle$.

Composition steps

- Compute $d = \gcd(u_1, u_2, v_1 + v_2 + h)$ and s_i such that $d = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2 + h)$.
- Set $u_3 := u_1 u_2 / d^2$

$$v_3 := \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \pmod{u_3}$$

Reduction steps

- **while** $\deg(u_3) > g$ **do:**

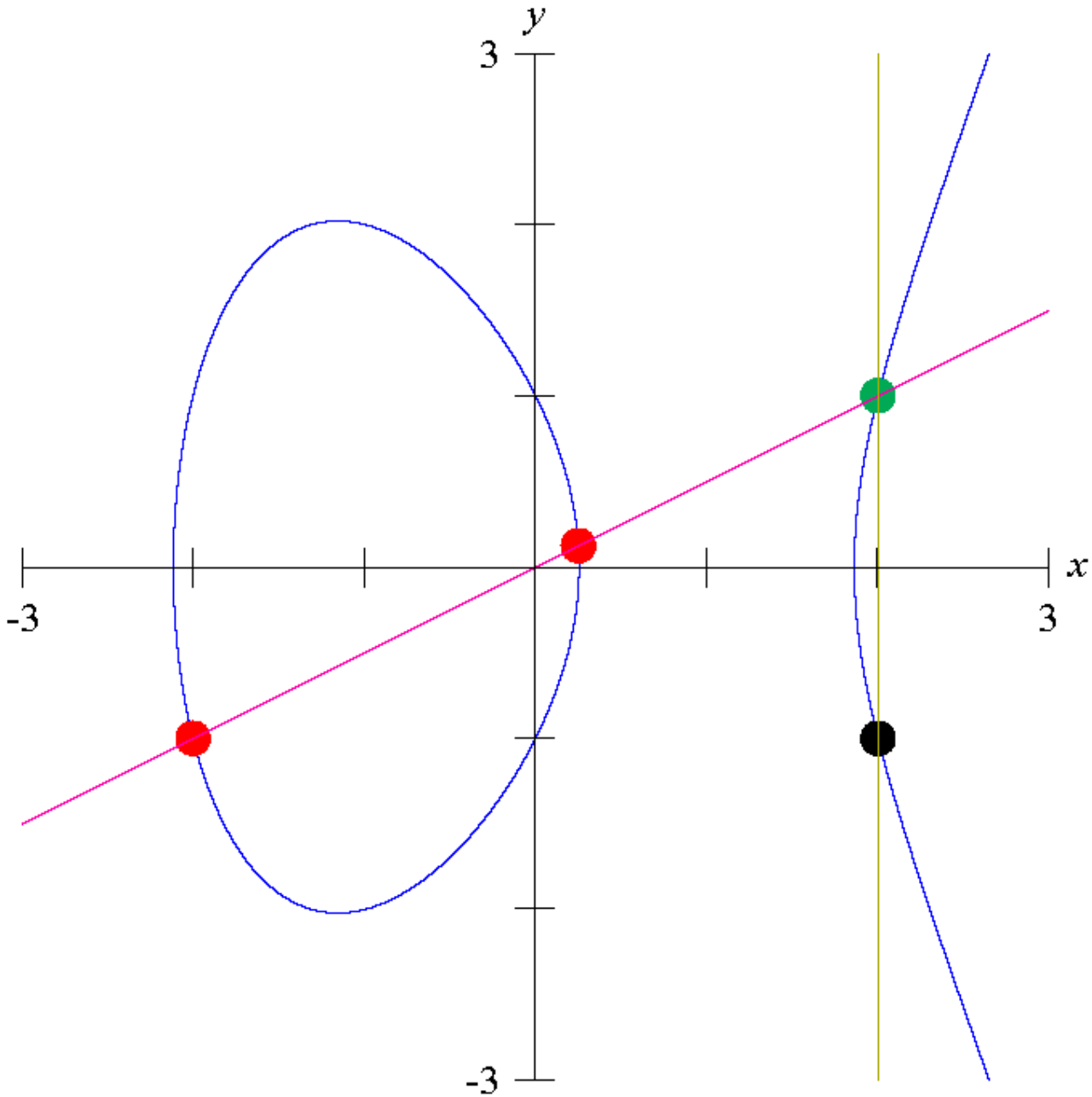
  $u_3 := (f - v_3 h - v_3^2)/u_3$

  $v_3 := -h - v_3 \pmod{u_3}$

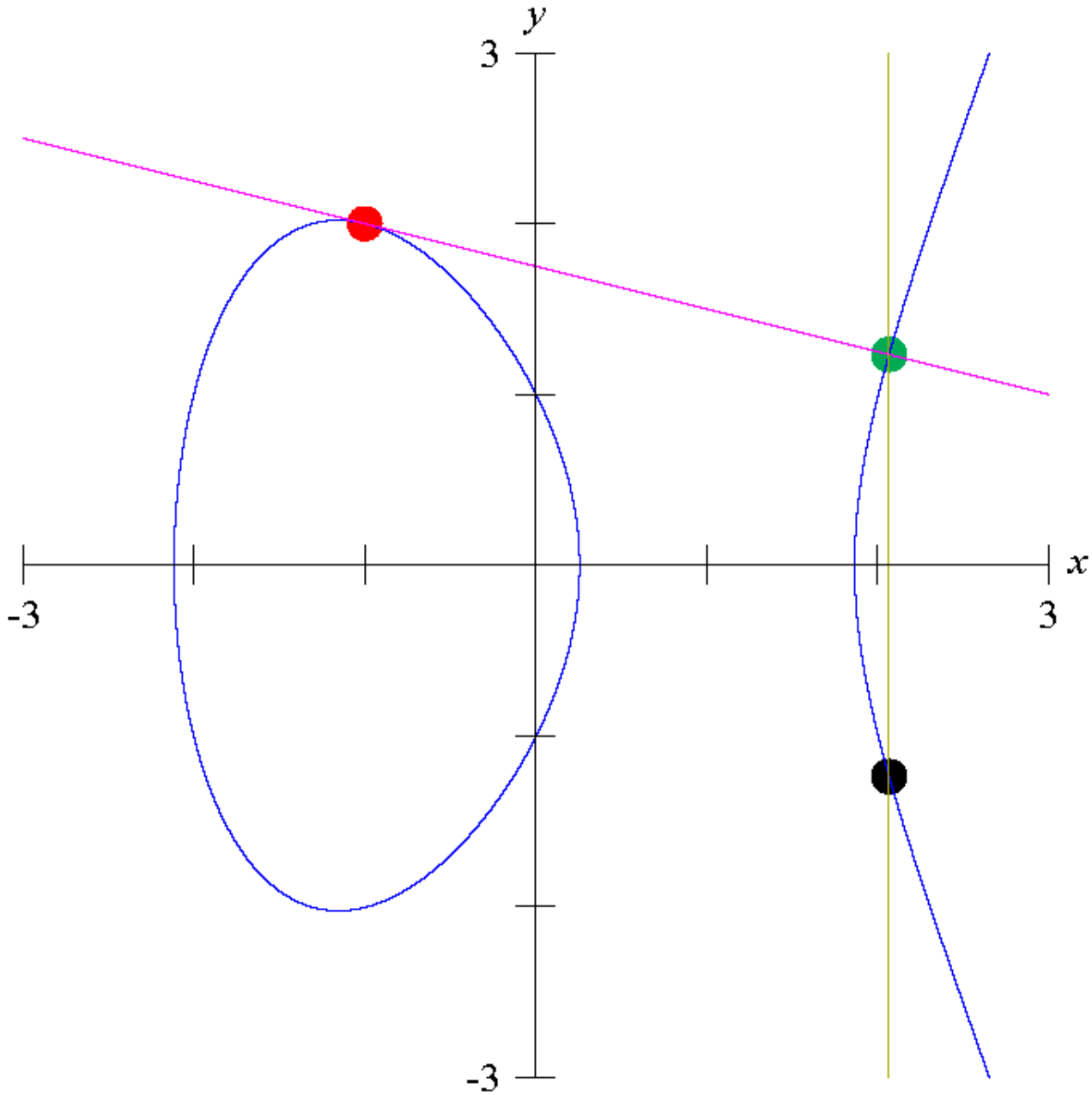
  end while
- Make u_3 monic (divide by leading coefficient)
- return $\langle u_3, v_3 \rangle$.

$\Longrightarrow$ Cantor's algorithm is liable to crash if K is not a field (eg. $K = \mathbb{Z}/N\mathbb{Z}$ with N composite). This is a good thing!

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



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



The discrete logarithm problem (DLP)

Let $(G, \oplus)$ be a finite abelian group.

DLP: Given $h \in \langle g \rangle \trianglelefteq G$, find $n \in \mathbb{Z}$ such that

$$[n]g := \overbrace{g + \ldots + g}^{n \text{ times}} = h$$

This is used in Diffie-Hellman key exchange.

Diffie-Hellman key exchange

Suppose Alice and Bob want to set up a shared secret key in order to communicate securely without Eve eavesdropping.
Public parameters: $(G, \oplus, P)$ where $P \in G$ has large (prime) order.

Diffie-Hellman key exchange

Suppose Alice and Bob want to set up a shared secret key in order to communicate securely without Eve eavesdropping.
Public parameters: $(G, \oplus, P)$ where $P \in G$ has large (prime) order.

Alice	Eve	Bob
chooses $a \in \mathbb{Z}$ at random		chooses $b \in \mathbb{Z}$ at random
computes $P_A = [a]P$		computes $P_B = [b]P$
receives P_B		receives P_A
computes $[a]P_B = [ab]P$	$=$	computes $[b]P_A = [ab]P$

Diffie-Hellman key exchange

Suppose Alice and Bob want to set up a shared secret key in order to communicate securely without Eve eavesdropping.
Public parameters: $(G, \oplus, P)$ where $P \in G$ has large (prime) order.

Alice	Eve	Bob
chooses $a \in \mathbb{Z}$ at random		chooses $b \in \mathbb{Z}$ at random
computes $P_A = [a]P$		computes $P_B = [b]P$
receives P_B	$\leftarrow$ $\rightarrow$	receives P_A
computes $[a]P_B = [ab]P$	$=$	computes $[b]P_A = [ab]P$

- Want DLP to be difficult to solve in G so that Eve cannot retrive a, b, ab from the transmission.
- We also need scalar multiplication in G to be efficient (relative to $\#G$).

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	$2^4 \cdot 211 \cdot 1289 \cdot 737177344105848850704770 47 \cdot 5370172597172987672353340036488640083$

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. How hard is DLP?

Attacking the DLP

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.

Attacking the DLP

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: $\widetilde{O}(q^{2-2/g}) < O(q^{g/2})$.

Attacking the DLP

Other groups

For the "well understood" groups $(\mathbb{Z}/N\mathbb{Z})^*$ and $\mathbb{F}_q^*$ there are subexponential algorithms known to solve DLP (index calculus).

This leaves us with hyperelliptic curves of genus 1 and 2 for use in cryptography.

Factorization algorithms

We list a few factorization algorithms and their heuristic expected runtimes:

Quadratic sieve	$L_N[1/2, 1]$
General number field sieve	$L_N[1/3, 1.09]$
Pollard's rho method	$O(\sqrt{p})$
Pollard's $p-1$ method	$O(p')$
Elliptic curve method	$L_p[1/2, \sqrt{2}]$

With the following notation:

- N is the number to be factored
- $L_x[\gamma, c] := \exp\left((c + o(1))(\log x)^{\gamma}(\log\log x)^{1-\gamma}\right)$ interpolates between polynomial and exponential complexity
- p is the smallest prime factor of N
- p' is the largest prime divisor of $p-1$

Pollard's $p-1$ method

Defn: An integer $N = \prod p_i^{e_i}$ is B-powersmooth if $p_i^{e_i} \leq B$ for all i.

Pollard's $p-1$ method finds prime factors p of N for which $p-1$ is powersmooth.
Let $a \in \mathbb{Z}$ satisfying $\gcd(a, N) = 1$.

Pollard's $p-1$ method

Defn: An integer $N = \prod p_i^{e_i}$ is B-powersmooth if $p_i^{e_i} \leq B$ for all i.

Pollard's $p-1$ method finds prime factors p of N for which $p-1$ is powersmooth.
Let $a \in \mathbb{Z}$ satisfying $\gcd(a, N) = 1$.
By Fermat's little theorem:

$$\text{if } \ (p-1) \mid m \ \text{ then } \ a^m \equiv 1 \pmod{p}.$$

Pollard's $p-1$ method

Defn: An integer $N = \prod p_i^{e_i}$ is B-powersmooth if $p_i^{e_i} \leq B$ for all i.

Pollard's $p-1$ method finds prime factors p of N for which $p-1$ is powersmooth.
Let $a \in \mathbb{Z}$ satisfying $\gcd(a, N) = 1$.
By Fermat's little theorem:

$$\text{if } \ (p-1) \mid m \ \text{ then } \ a^m \equiv 1 \pmod{p}.$$

Assume that $p-1$ is B-powersmooth then take $m = \operatorname{lcm}(1, \ldots, B)$ so

$$(p-1) \mid m \implies p \mid (a^m - 1)$$

together with $p \mid N$ implies that $p \mid \gcd(a^m - 1, N) > 1$.

Pollard's $p-1$ method

The algorithm

Given as input: N to be factored and a powersmooth bound B

- Choose a random $a \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(a, N) = 1$
- Compute $m = \mathrm{lcm}(1, \ldots, B)$
- Return $g = \gcd(a^m - 1, N)$.

If $p-1$ is B-powersmooth, the output g is a nontrivial factor of N.

Pollard's $p-1$ method

The algorithm

Given as input: N to be factored and a powersmooth bound B

- Choose a random $a \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(a, N) = 1$
- Compute $m = \mathrm{lcm}(1, \ldots, B)$
- Return $g = \gcd(a^m - 1, N)$.

If $p-1$ is B-powersmooth, the output g is a nontrivial factor of N.
If $g = 1$, try again with a larger value for B.
If $g = N$, try again with a smaller (or equal) value for B,
otherwise try again with a different value of a or higher value for B.

Pollard's $p-1$ method

Good example

Let's factorize $N = 7663$ with $B = 13$:

$m = \operatorname{lcm}(1, \ldots, 13) = 360360$

Take $a = 2$. We have

$$2^{360360} - 1 \equiv 4266 \pmod{N}$$

and so

$$\gcd(a^m - 1, N) = \gcd(4266, 7663) = 79$$

and $N = 79 \cdot 97$.

This works because $79 - 1 = 2 \cdot 3 \cdot 13$ is 13-powersmooth.

Pollard's $p-1$ method

Why it works

$(\mathbb{Z}/7663\mathbb{Z})^*$	$(\mathbb{Z}/79\mathbb{Z})^*$ has order 78	$(\mathbb{Z}/97\mathbb{Z})^*$ has order 96
$a = 35$	35	35

Pollard's $p-1$ method

Why it works

$(\mathbb{Z}/7663\mathbb{Z})^*$	$(\mathbb{Z}/79\mathbb{Z})^*$ has order 78	$(\mathbb{Z}/97\mathbb{Z})^*$ has order 96
$a = 35$	35	35
$a^2 = 1225$	40	61

Pollard's $p-1$ method

Why it works

$(\mathbb{Z}/7663\mathbb{Z})^*$	$(\mathbb{Z}/79\mathbb{Z})^*$ has order 78	$(\mathbb{Z}/97\mathbb{Z})^*$ has order 96
$a = 35$	35	35
$a^2 = 1225$	40	61
$a^3 = 4560$	57	1

Pollard's $p-1$ method

Why it works

$(\mathbb{Z}/7663\mathbb{Z})^*$	$(\mathbb{Z}/79\mathbb{Z})^*$ has order 78	$(\mathbb{Z}/97\mathbb{Z})^*$ has order 96
$a = 35$	35	35
$a^2 = 1225$	40	61
$a^3 = 4560$	57	1
	$a^{78} = 1$	$a^3 = 1$

$a^3 = 1$ in $(\mathbb{Z}/97\mathbb{Z})^*$ but $a^3 \neq 1$ in $(\mathbb{Z}/77\mathbb{Z})^*$

Pollard's $p-1$ method

Why it works

$(\mathbb{Z}/7663\mathbb{Z})^*$	$(\mathbb{Z}/79\mathbb{Z})^*$ has order 78	$(\mathbb{Z}/97\mathbb{Z})^*$ has order 96
$a = 35$	35	35
$a^2 = 1225$	40	61
$a^3 = 4560$	57	1
	$a^{78} = 1$	$a^3 = 1$

$a^3 = 1$ in $(\mathbb{Z}/97\mathbb{Z})^*$ but $a^3 \neq 1$ in $(\mathbb{Z}/77\mathbb{Z})^*$

$\Longrightarrow a^3 \neq 1$ in $(\mathbb{Z}/7663\mathbb{Z})^*$ and so $\gcd(a^3 - 1, 7663)$ gives us something nontrivial (namely 97).

Pollard's $p-1$ method

Bad example

Consider trying to factorize $N = 6313 = 59 \cdot 107$

Although this number is roughly the same size as our previous example ($N = 79 \cdot 97, B = 13$) the smallest B that works in this example is $B = 29$.
The problem is that the largest prime divisors of $p-1$ are "big".

- There is $\approx (1/k)^k$ probability of success if $B = O(N^{1/2k})$.
- The property that $p-1$ is B-smooth restricts the practicality of the algorithm to finding "small" prime factors ($\lesssim 10^{12}$ with $B \approx 10^6$).

Pollard's $p-1$ method

Bad example

Consider trying to factorize $N = 6313 = 59 \cdot 107$

Although this number is roughly the same size as our previous example ($N = 79 \cdot 97, B = 13$) the smallest B that works in this example is $B = 29$.
The problem is that the largest prime divisors of $p-1$ are "big".

What if we could replace $p - 1 = \#(\mathbb{Z}/p\mathbb{Z})^*$ with a group of size $p - 2$?
In the above example, $107 - 2 = 105 = 3 \cdot 5 \cdot 7$ which is 7-smooth!
For example, the elliptic curve

$$E: \ y^2 = x^3 + 79x + 56$$

has cardinality $\#E(\mathbb{Z}/107\mathbb{Z}) = 105$.
Well, we can!

Elliptic curve method (ECM)

The algorithm

Given as input: N to be factored and a powersmooth bound B.

1. Pick a random "elliptic curve" over $\mathbb{Z}/N\mathbb{Z}$ given by an equation $y^2 = x^3 + ax + b$ and pick a point $P = (x, y)$ on it.
2. Attempt to compute $[m]P$ where $m = \operatorname{lcm}(1, \ldots, B)$.
   If this fails then we detect a zero divisor $g \in \mathbb{Z}/N\mathbb{Z}$. If $g = N$ or if $[m]P$ succeeds, go back to Step 1.

Elliptic curve method (ECM)

Example

$E(\mathbb{Z}/6313\mathbb{Z})$: $y^2 = x^3 + 79x + 56$	$E(\mathbb{Z}/59\mathbb{Z})$ has order 48	$E(\mathbb{Z}/107\mathbb{Z})$ has order 105
$P = (47, 4863)$	$(47, 25)$	$(47, 48)$

Elliptic curve method (ECM)

Example

$E(\mathbb{Z}/6313\mathbb{Z})$: $y^2 = x^3 + 79x + 56$	$E(\mathbb{Z}/59\mathbb{Z})$ has order 48	$E(\mathbb{Z}/107\mathbb{Z})$ has order 105
$P = (47, 4863)$	$(47, 25)$	$(47, 48)$
$[2]P = (-167, 2627)$	$(10, 31)$	$(47, 59)$

Elliptic curve method (ECM)

Example

$E(\mathbb{Z}/6313\mathbb{Z})$: $y^2 = x^3 + 79x + 56$	$E(\mathbb{Z}/59\mathbb{Z})$ has order 48	$E(\mathbb{Z}/107\mathbb{Z})$ has order 105
$P = (47, 4863)$	$(47, 25)$	$(47, 48)$
$[2]P = (-167, 2627)$	$(10, 31)$	$(47, 59)$
$[3]P$ fails	$(5, 24)$	∞

Elliptic curve method (ECM)

Example

$E(\mathbb{Z}/6313\mathbb{Z})$: $y^2 = x^3 + 79x + 56$	$E(\mathbb{Z}/59\mathbb{Z})$ has order 48	$E(\mathbb{Z}/107\mathbb{Z})$ has order 105
$P = (47, 4863)$	$(47, 25)$	$(47, 48)$
$[2]P = (-167, 2627)$	$(10, 31)$	$(47, 59)$
$[3]P$ fails	$(5, 24)$	∞
	$[16]P = 0$	$[3]P = 0$

The gradient of the line through P and $[2]P$ has denominator $47 - (-167) = 214$ and $\gcd(214, 6313) = 107 > 1$.

The advantage of ECM is that

$$\#E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - t \text{ where } |t| < 2\sqrt{p}.$$

Moreover, every possible value for t in this range can occur.

The advantage of ECM is that

$$\#E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - t \text{ where } |t| < 2\sqrt{p}.$$

Moreover, every possible value for t in this range can occur.

Example: $(p = 59)$: $|t| < 2\sqrt{p} \approx 15.36...$ and of the integers in $[59 - 15, 59 + 15]$ the best number is $60 = 2^2 \cdot 3 \cdot 5$ which is 5-powersmooth. So ECM can detect 59 with $B = 5$.

The advantage of ECM is that

$$\#E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - t \text{ where } |t| < 2\sqrt{p}.$$

Moreover, every possible value for t in this range can occur.

Example: $(p = 59)$: $|t| < 2\sqrt{p} \approx 15.36...$ and of the integers in $[59 - 15, 59 + 15]$ the best number is $60 = 2^2 \cdot 3 \cdot 5$ which is 5-powersmooth. So ECM can detect 59 with $B = 5$.

- There are sufficiently many smooth numbers in intervals of the form $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$ to make ECM a subexponential algorithm.
- Although not as fast as GNFS, ECM is commonly used to detect prime factors of size $\lesssim 10^{20}$ with $B \approx 10^4$.

Hyperelliptic curve method (HECM)

From ECM to HECM

One can replace elliptic curves with hyperelliptic curves:

$$\begin{array}{rcl} \text{ECM} & \dashrightarrow & \text{HECM (genus } 2) \\ E & \dashrightarrow & J_H \\ \text{runtime: } L_p[1/2, \sqrt{2}] & \dashrightarrow & L_p[2/3, c](\log N)^2 \end{array}$$

Theoretically, the algorithm is identical, but there are some practical obstacles to overcome:

- The group operations on J_H are slower than for E
- $\#J_H(\mathbb{F}_p) \approx p^2$ whereas $\#E(\mathbb{F}_p) \approx p$.
  (Larger numbers are less likely to be powersmooth)

These obstacles have been tackled recently by R. Cosset ["Factorization with genus 2 curves", Math. Comp. 2010]

HECM improvements

Kummer surfaces

$J_H/\langle[-1]\rangle \xrightarrow{\psi} \mathcal{K}$ is isomorphic to a Kummer surface $\mathcal{K}$ in $\mathbb{P}^3$:

$$\mathcal{K}: \ (x^4+y^4+z^4+t^4)+2Exyzt-F(x^2t^2+y^2z^2) \\ -G(x^2z^2+y^2t^2)H(x^2y^2+z^2t^2)=0$$

Arithmetic on J_H partially transfers across to $\mathcal{K}$:

- (Double). Given $P=\psi(D)\in\mathcal{K}$ one can compute $\psi([2]D)=:[2]P$ on $\mathcal{K}$

HECM improvements

Kummer surfaces

$J_H/\langle[-1]\rangle \xrightarrow{\psi} \mathcal{K}$ is isomorphic to a Kummer surface $\mathcal{K}$ in $\mathbb{P}^3$:

$$\mathcal{K}: \ (x^4+y^4+z^4+t^4)+2Exyzt-F(x^2t^2+y^2z^2) \\ -G(x^2z^2+y^2t^2)H(x^2y^2+z^2t^2)=0$$

Arithmetic on J_H partially transfers across to $\mathcal{K}$:

- (Double). Given $P=\psi(D)\in\mathcal{K}$ one can compute $\psi([2]D)=:[2]P$ on $\mathcal{K}$
- (Pseudo-add). Given $P=\psi(D)$ and $Q=\psi(D')$ we cannot distinguish $\psi(D+D')$ from $P=\psi(D-D')$. However knowing one value $P-Q$ determines the other $P+Q$.

HECM improvements

Kummer surfaces

$J_H/\langle[-1]\rangle \xrightarrow{\psi} \mathcal{K}$ is isomorphic to a Kummer surface $\mathcal{K}$ in $\mathbb{P}^3$:

$$\mathcal{K}: \ (x^4+y^4+z^4+t^4)+2Exyzt-F(x^2t^2+y^2z^2) \\ -G(x^2z^2+y^2t^2)H(x^2y^2+z^2t^2)=0$$

Arithmetic on J_H partially transfers across to $\mathcal{K}$:

- (Double). Given $P=\psi(D)\in\mathcal{K}$ one can compute $\psi([2]D)=:[2]P$ on $\mathcal{K}$
- (Pseudo-add). Given $P=\psi(D)$ and $Q=\psi(D')$ we cannot distinguish $\psi(D+D')$ from $P=\psi(D-D')$. However knowing one value $P-Q$ determines the other $P+Q$.
- Scalar multiplication can be derived from double and pseudo-add algorithms.

Fact: Scalar multiplication is faster on $\mathcal{K}$ than on J_H.

HECM improvements

Choosing the right hyperelliptic curves

To address the smoothness problem, use decomposable Jacobians

$$J_H \overset{\text{isogeny}}{\longrightarrow} E_1 \times E_2.$$

In this case,

$$\#J_H(\mathbb{Z}/p\mathbb{Z}) \;=\; \#E_1(\mathbb{Z}/p\mathbb{Z}) \cdot \#E_2(\mathbb{Z}/p\mathbb{Z}).$$

There are 2-dimensional families of hyperelliptic curves with decomposable Jacobians.

- Cosset uses a "nice" subfamily of $((2,2)$-decomposable) hyperelliptic curves for which Kummer surface arithmetic is fast.
- One run of HECM "equals" two simultaneous runs of ECM.

The end

So perhaps HECM isn't as bad as it looks!

Quadratic sieve	$L_N[1/2, 1]$
General number field sieve	$L_N[1/3, 1.09]$
Pollard's rho method	$O(\sqrt{p})$
Pollard's $p-1$ method	$O(p')$
ECM	$L_p[1/2, \sqrt{2}]$
HECM genus 2	$L_p[2/3, c](\log N)^2$

Thanks for listening!