Hyperelliptic curve reduction

Florian Bouyer[1] Marco Streng[2]

[1]University of Warwick, www.warwick.ac.uk/fbouyer
[2]Universiteit Leiden, www.math.leidenuniv.nl/~streng

Warwick Postgraduate Seminar, 1st Oct 2014

1. *Introduction*
   - Elliptic Curves
   - Hyperelliptic Curves

2. *Reduction*
   - Reducing Discriminant
   - Stoll-Cremona Reduction

3. *General Number Fields*
   - How to extend of a number field
   - Our tables

Elliptic Curves

We are going to be working over $\mathbb{Q}$

Definitions

An *elliptic curve* (over $\mathbb{Q}$) is an equation of the form

$$E : y^2 = x^3 + ax + b, \ (4a^3 + 27b^2 \neq 0)$$

The *j-invariant* of E is

$$j(E) = \frac{4a^3}{4a^3 + 27b^2}$$

We are going to be working over $\mathbb{Q}$

Definitions

An *elliptic curve* (over $\mathbb{Q}$) is an equation of the form

$$E : y^2 = x^3 + ax + b, \ (4a^3 + 27b^2 \neq 0)$$

The *j-invariant* of E is

$$j(E) = \frac{4a^3}{4a^3 + 27b^2}$$

Theorem

$$E \cong_{\overline{\mathbb{Q}}} E' \iff j(E) = j(E')$$

Given $j \in \mathbb{Q}$, let

$$E_j : y^2 = x^3 + ax + a, \text{ where } a = \frac{27}{4}\frac{j}{(1728 - j)}$$

$$E_0 : y^2 = x^3 - 1,\ E_{1728} : y^2 = x^3 + x$$

then

$$j(E_j) = j$$

Example

Let $E : y^2 = x^3 + 8x + 16$, then $j(E) = 13824/35$ and $E_j : y^2 = x^3 + 2x + 2$. Note $E \to E_j$ by $(x, y) \mapsto (2x, \sqrt{8}y)$:

$$\left(\sqrt{8}y\right)^2 = (2x)^3 + 8\,(2x) + 16$$

$$8y^2 = 8x^3 + 16x + 16$$

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

Given $j \in \mathbb{Q}$, let

$$E_j : y^2 = x^3 + ax + a, \text{ where } a = \frac{27}{4}\frac{j}{(1728 - j)}$$

$$E_0 : y^2 = x^3 - 1,\ E_{1728} : y^2 = x^3 + x$$

then

$$j(E_j) = j$$

Example

Let $E : y^2 = x^3 + 8x + 16$, then $j(E) = 13824/35$ and $E_j : y^2 = x^3 + 2x + 2$. Note $E \to E_j$ by $(x, y) \mapsto (2x, \sqrt{8}y)$:

$$\left(\sqrt{8}y\right)^2 = (2x)^3 + 8\,(2x) + 16$$

$$8y^2 = 8x^3 + 16x + 16$$

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

```
sage: EllipticCurve_from_j(13824/35)
Elliptic Curve defined by y^2 = x^3 + 8*x - 16 over Rationa
```

Definition

A (genus 2) *hyperelliptic curve* (over $\mathbb{Q}$), C, is a curve of the form $y^2 = f(x)$, with $f(x) \in \mathbb{Q}[x]$ of degree 5 or 6 and having distinct roots.

$C_f : y^2 = f(x)$, $C_F : Y^2 = F(X, Z)$ where

$$F(X, Z) = Z^6 f(X/Z)$$

is a binary form of degree 6. Note $f(x) = F(x, 1)$.

For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$, let

$$F \circ A = F(aX + bZ, cX + dZ) \ , \ f \cdot A = f\left(\frac{ax + b}{cx + d}\right)$$

and for $u \in \mathbb{Q}^*$, then uF is just scalar multiplication. Then (under one assumption)

$$C_F \cong C_{F'} \iff F \sim_{(\mathrm{GL}_2(\mathbb{Q}) * \mathbb{Q}^*)} F'$$

Igusa-Clebsch Invariants

Recall that for elliptic curves, the j-invariant told us when two curves where isomorphic.

Can a similar invariant be defined for hyperelliptic curves?

Igusa-Clebsch Invariants

Recall that for elliptic curves, the j-invariant told us when two curves where isomorphic.

Can a similar invariant be defined for hyperelliptic curves?

Yes. The Igusa-Clebsch invariants: polynomials I_2, I_4, I_6, I_{10} in the coefficients of f.

Theorem

$$C \cong_{\overline{\mathbb{Q}}} C' \iff I_n(C) = u^n I_n(C') \forall n \text{ for some } u \in \overline{\mathbb{Q}}^*$$

Not as nice as j

Given $f = a_6 \prod_{i=1}^{6}(x - \alpha_i)$, let

$$I_{10} = a_6^{10} \prod_{i<j} (\alpha_i - \alpha_j)^2 = \Delta(f)$$

Use (ij) do denote $(\alpha_i - \alpha_j)$ and take the following sum over the S_6-orbit

$$I_2 = a_6^2 \sum_{15\,\text{terms}} (12)^2(34)^2(56)^2$$

$$I_4 = a_6^4 \sum_{10\,\text{terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2$$

$$I_6 = a_6^6 \sum_{60\,\text{terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2$$

Not as nice as j

Given $f = a_6 \prod_{i=1}^{6}(x - \alpha_i)$, let

$$I_{10} = a_6^{10} \prod_{i<j} (\alpha_i - \alpha_j)^2 = \Delta(f)$$

Use (ij) do denote $(\alpha_i - \alpha_j)$ and take the following sum over the S_6-orbit

$$I_2 = a_6^2 \sum_{15\,\text{terms}} (12)^2(34)^2(56)^2$$

$$I_4 = a_6^4 \sum_{10\,\text{terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2$$

$$I_6 = a_6^6 \sum_{60\,\text{terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2$$

```
sage: P.<x> = QQ[]
sage: H = HyperellipticCurve(x^6 + x^2 + 10*x + 2014)
sage: ic = H.igusa_clebsch_invariants(); ic
(-7733760, 1682185617408, -40112994226752061 44,
-16210812163577704090752153 6)
```

Igusa-Clebsch Invariants

Recall that for elliptic curves, the j-invariant told us when two curves where isomorphic.

Can a similar invariant be defined for hyperelliptic curves?

Yes. The Igusa-Clebsch invariants: polynomials I_2, I_4, I_6, I_{10} in the coefficients of f.

Igusa-Clebsch Invariants

Recall that for elliptic curves, the j-invariant told us when two curves where isomorphic.

Can a similar invariant be defined for hyperelliptic curves?

Yes. The Igusa-Clebsch invariants: polynomials I_2, I_4, I_6, I_{10} in the coefficients of f.

Recall that for elliptic curves, we could construct an elliptic curve of a given j-invariant

Can we construct an hyperelliptic curve with given I_2, I_4, I_6 and I_{10}?

Igusa-Clebsch Invariants

Recall that for elliptic curves, the j-invariant told us when two curves where isomorphic.

Can a similar invariant be defined for hyperelliptic curves?

Yes. The Igusa-Clebsch invariants: polynomials I_2, I_4, I_6, I_{10} in the coefficients of f.

Recall that for elliptic curves, we could construct an elliptic curve of a given j-invariant

Can we construct an hyperelliptic curve with given I_2, I_4, I_6 and I_{10}?

Yes (sometimes). Mestre's algorithm (1991)

Igusa-Clebsch Invariants

Recall that for elliptic curves, the j-invariant told us when two curves where isomorphic.

Can a similar invariant be defined for hyperelliptic curves?

Yes. The Igusa-Clebsch invariants: polynomials I_2, I_4, I_6, I_{10} in the coefficients of f.

Recall that for elliptic curves, we could construct an elliptic curve of a given j-invariant

Can we construct an hyperelliptic curve with given I_2, I_4, I_6 and I_{10}?

Yes (sometimes). Mestre's algorithm (1991)

Mestre's Algorithm either returns such an hyperelliptic curve, or it warn us that there exists no hyperelliptic curves over $\mathbb{Q}$ with such Igusa-Clebsch invariants

We implemented this in Sage

```
sage: P.<x> = QQ[]
sage: H = HyperellipticCurve(x^6 + x^2 + 10*x + 2014)
sage: ic = H.igusa_clebsch_invariants(); ic
(-7733760, 1682185617408, -401129942267520614 4,
-16210812163577704091075215 36)
```

Apply Mestre's algorithm to the invariants to get:

$$
\begin{aligned}
y^2 = \; & -65890115389444619461768881430333818525798363760055174986370043922147227 38x^6 \\
& -38435900644556699749978359126497610242219924318937118411816122280433019178x^5 \\
& -93420591846174958060380647391685883668736557612142778838618560899251216495x^4 \\
& -12110076721033490531775952881258348621323649747176251911102719258810912896 0x^3 \\
& -88302642759265185238698246881065772575189911318959884317018575874280688620x^2 \\
& -34339916629287535811248104831570691742058201032248166495092985792535971878x \\
& -55643383428214857442929970460022416257672886098225061094634476746825390 38
\end{aligned}
$$

```
sage: P.<x> = QQ[]
sage: H = HyperellipticCurve(x^6 + x^2 + 10*x + 2014)
sage: ic = H.igusa_clebsch_invariants(); ic
(-7733760, 1682185617408, -401129942267520614 4,
-16210812163577704091075215 36)
```

Apply Mestre's algorithm to the invariants to get:

$$
\begin{aligned}
y^2 = \; & -65890115389444619461768881430333818525798363760055174986370043922147227 38x^6 \\
& -38435900644556699749978359126497610242219924318937118411816122280433019178x^5 \\
& -93420591846174958060380647391685883668736557612142778838618560899251216495x^4 \\
& -12110076721033490531775952881258348621323649747176251911102719258810912896 0x^3 \\
& -88302642759265185238698246881065772575189911318959884317018575874280688620x^2 \\
& -34339916629287535811248104831570691742058201032248166495092985792535971878x \\
& -55643383428214857442929970460022416257672886098225061094634476746825390 38
\end{aligned}
$$

The coefficients are horrible and in no way practical!

Apply Mestre's algorithm to the invariants to get

$$\begin{aligned} y^2 = & -6589011538944461946176888143033381852579836376005517498637004392214722738x^6 \\ & -384359006445566997499783591264976102422199243189371184118161222804330191 78x^5 \\ & -934205918461749580603806473916858836687365576121427788386185608992512164 95x^4 \\ & -121100767210334905317759528812583486213236497471762519111027192588109128960x^3 \\ & -883026427592651852386982468810657725751899113189598843170185758742806886 20x^2 \\ & -343399166292875358112481048315706917420582010322481664950929857925359718 78x \\ & -556433834282148574429299704600224162576728860982250610946344767468253903 8 \end{aligned}$$

The coefficients are horrible and in no way practical!
But wait! The coefficients have non-trivial gcd of
$-2015071^3 \cdot 287147292790 13^3$

Apply Mestre's algorithm to the invariants to get

$$
\begin{aligned}
y^2 = \; & -6589011538944461946176888143033381852579836376005517498637004392214722738x^6 \\
& -384359006445566997499783591264976102422199243189371184118161222804330191 78x^5 \\
& -934205918461749580603806473916858836687365576121427788386185608992512164 95x^4 \\
& -121100767210334905317759528812583486213236497471762519111027192588109128960x^3 \\
& -883026427592651852386982468810657725751899113189598843170185758742806886 20x^2 \\
& -343399166292875358112481048315706917420582010322481664950929857925359718 78x \\
& -556433834282148574429299704600224162576728860982250610946344767468253903 8
\end{aligned}
$$

The coefficients are horrible and in no way practical!
But wait! The coefficients have non-trivial gcd of
$-2015071^3 \cdot 287147292790 13^3$

$$
\begin{aligned}
y^2 = \; & 34012224032614x^6 + 198404640193934x^5 \\
& +482233500480485x^4 + 625117500634880x^3 \\
& +455814844221860x^2 + 177261328312034x \\
& +28722900421514
\end{aligned}
$$

Apply Mestre's algorithm to the invariants to get

$$\begin{aligned} y^2 = & -6589011538944461946176888143033381852579836376005517498637004392214722738x^6 \\ & -384359006445566997499783591264976102422199243189371184118161222804330191 78x^5 \\ & -93420591846174958060380647391685883668736557612142778838618560899251216495x^4 \\ & -12110076721033490531775952881258348621323649747176251911102719258810912896 0x^3 \\ & -88302642759265185238698246881065772575189911318959884317018575874280688620x^2 \\ & -34339916629287535811248104831570691742058201032248166495092985792535971878x \\ & -55643383428214857442929970460022416257672886098225061094634476746825390 38 \end{aligned}$$

The coefficients are horrible and in no way practical!
But wait! The coefficients have non-trivial gcd of
$-2015071^3 \cdot 287147292790 13^3$

$$\begin{aligned} y^2 = & \ 34012224032614x^6 + 198404640193934x^5 \\ & +482233500480485x^4 + 625117500634880x^3 \\ & +455814844221860x^2 + 177261328312034x \\ & +28722900421514 \end{aligned}$$

Goal: Given an hyperelliptic curve C over $\mathbb{Q}$, we want to find a "small" hyperelliptic curve C' over $\mathbb{Q}$ such that $C \cong_{\overline{\mathbb{Q}}} C'$.

Reduction

Recall: $C_F : Y^2 = F(X, Z)$.

Given $[A, u] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right] \in \mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*$, let

$$F' = F \cdot [A, u] := u \cdot F \circ A \quad \text{where } F \circ A = F(aX + bZ, cX + dZ)$$

Goal: Given F, we want to find a "small" element of its $(\mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*)$-orbit

Reduction

Recall: $C_F : Y^2 = F(X, Z)$.

Given $[A, u] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right] \in \mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*$, let

$$F' = F \cdot [A, u] := u \cdot F \circ A \quad \text{where } F \circ A = F(aX + bZ, cX + dZ)$$

Goal: Given F, we want to find a "small" element of its $(\mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*)$-orbit

"Small" means

Coefficients are in $\mathbb{Z}$

Reduction

Recall: $C_F : Y^2 = F(X, Z)$.

Given $[A, u] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right] \in \mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*$, let

$$F' = F \cdot [A, u] := u \cdot F \circ A \quad \text{where } F \circ A = F(aX + bZ, cX + dZ)$$

Goal: Given F, we want to find a "small" element of its $(\mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*)$-orbit

"Small" means

Coefficients are in $\mathbb{Z}$

The discriminant $\Delta(f)$ has small norm (absolute value)

Reduction

Recall: $C_F : Y^2 = F(X, Z)$.

Given $[A, u] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right] \in \mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*$, let

$$F' = F \cdot [A, u] := u \cdot F \circ A \quad \text{where } F \circ A = F(aX + bZ, cX + dZ)$$

Goal: Given F, we want to find a "small" element of its $(\mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*)$-orbit

"Small" means

Coefficients are in $\mathbb{Z}$

The discriminant $\Delta(f)$ has small norm (absolute value)

The coefficients are "small" (recursive definition?!)

Reduction

Recall: $C_F : Y^2 = F(X, Z)$.

Given $[A, u] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right] \in \mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*$, let

$$F' = F \cdot [A, u] := u \cdot F \circ A \quad \text{where } F \circ A = F(aX + bZ, cX + dZ)$$

Goal: Given F, we want to find a "small" element of its $(\mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*)$-orbit

"Small" means

- Coefficients are in $\mathbb{Z}$
  - Scaling
- The discriminant $\Delta(f)$ has small norm (absolute value)

- The coefficients are "small" (recursive definition?!)

Reduction

Recall: $C_F : Y^2 = F(X, Z)$.

Given $[A, u] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right] \in \mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*$, let

$$F' = F \cdot [A, u] := u \cdot F \circ A \quad \text{where } F \circ A = F(aX + bZ, cX + dZ)$$

Goal: Given F, we want to find a "small" element of its $(\mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*)$-orbit

"Small" means

- Coefficients are in $\mathbb{Z}$
  - Scaling
- The discriminant $\Delta(f)$ has small norm (absolute value)
  - We deal with this locally (at each prime)
- The coefficients are "small" (recursive definition?!)

Reduction

Recall: $C_F : Y^2 = F(X, Z)$.

Given $[A, u] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right] \in \mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*$, let

$$F' = F \cdot [A, u] := u \cdot F \circ A \quad \text{where } F \circ A = F(aX + bZ, cX + dZ)$$

Goal: Given F, we want to find a "small" element of its $(\mathrm{GL}_2(\mathbb{Q}) \times \mathbb{Q}^*)$-orbit

"Small" means

- Coefficients are in $\mathbb{Z}$
  - Scaling
- The discriminant $\Delta(f)$ has small norm (absolute value)
  - We deal with this locally (at each prime)
- The coefficients are "small" (recursive definition?!)
  - The only freedom left is action by $\mathrm{GL}_2(\mathbb{Z}) \times \{\pm 1\}$

Local Reduction of $\Delta(f)$

Recall: Given a prime p, the valuation $v_p(x)$ for $x \in \mathbb{Z}$ is defined as the smallest $e \geq 0$ such that $p^{e+1} \nmid x$.
(Examples: $v_2(18) = 1, v_3(18) = 2, v_5(18) = 0$)
Given F, we want to find an element in the orbit $F \cdot (\mathrm{GL}_2(\mathbb{Z}) \times \mathbb{Q}^*)$ with $v_p(\Delta)$ minimal

Proposition (B-Streng(?))

Suppose $f \in \mathbb{Z}[x]$ of degree 5 or 6 ($2g+1$ or $2g+2$). (And $\mathrm{Aut}((C_f)_{\overline{\mathbb{Q}}}) = \{1, \iota\}$). Then f is non-minimal at p if and only if one of the following holds:

- *f is not primitive, that is, $f^\dagger := f/p$ is integral*
- *($f \mod p$) has a 4-fold root $\bar{t}$ mod p. Moreover, for every lift t, $f^\dagger := f(px+t)/p^4$ is integral. ($g+2$)*
- *$\deg(f \mod p) \leq 2$. Moreover, $f^\dagger := f(x/p)p^2$ is integral. ($n-2g$)*

In each case, we have $v_p(\Delta(f^\dagger)) < v_p(\Delta(f))$

Local Reduction of $\Delta(f)$

Proposition (B-Streng(?))

Suppose $f \in \mathbb{Z}[x]$ *of degree* 5 *or* 6 ($2g+1$ *or* $2g+2$). *(And* $\mathrm{Aut}((C_f)_{\overline{\mathbb{Q}}}) = \{1, \iota\}$*). Then* f *is non-minimal at* p *if and only if one of the following holds:*

- f *is not primitive, that is,* $f^\dagger := f/p$ *is integral*
- $(f \mod p)$ *has a 4-fold root* $\overline{t}$ *mod* p*. Moreover, for every lift* t*,* $f^\dagger := f(px+t)/p^4$ *is integral.* $(g+2)$
- $\deg(f \mod p) \leq 2$*. Moreover,* $f^\dagger := f(x/p)p^2$ *is integral.* $(n-2g)$

In each case, we have $v_p(\Delta(f^\dagger)) < v_p(\Delta(f))$

Note: To find if there is a fourth root, calculate $\gcd(\overline{f}, \overline{f}', \overline{f}'', \overline{f}''') = a_n(x-\overline{t})^n = \sum a_i x^i$. Then $\overline{t} = -a_{n-1}/(na_n)$. So repeating each of the above bullet points, we can reduce f until $v_p(\Delta(f))$ is minimal.

Global Reduction of $\Delta(f)$

If we know the prime factorisation of $\Delta(f)$, then the previous local algorithms gives a global algorithm.

Global Reduction of $\Delta(f)$

If we know the prime factorisation of $\Delta(f)$, then the previous local algorithms gives a global algorithm.
Do we need to factorise? It seems essential:
Let p and q be large unknown primes, $n = p^2 q$ and

$$f = n^2 x^6 + x + 1$$

this has $\Delta(f) = (5^2 - 6^6 n^2) n^8$
Let $g = f(x/p)p^2 = q^2 x^6 + px + p^2$ with
$\Delta(g) = (5^5 - 6^6 n^2) p^6 q^8 = \Delta(f)/p^{10}$
For most p and q, g is the minimal model.
If we can compute g, then we can find $p = \sqrt[10]{\Delta(f)/\Delta(g)}$ and factor n

Global Reduction of $\Delta(f)$

If we know the prime factorisation of $\Delta(f)$, then the previous local algorithms gives a global algorithm.
Do we need to factorise? It seems essential:
Let p and q be large unknown primes, $n = p^2q$ and

$$f = n^2x^6 + x + 1$$

this has $\Delta(f) = (5^2 - 6^6n^2)n^8$
Let $g = f(x/p)p^2 = q^2x^6 + px + p^2$ with
$\Delta(g) = (5^5 - 6^6n^2)p^6q^8 = \Delta(f)/p^{10}$
For most p and q, g is the minimal model.
If we can compute g, then we can find $p = \sqrt[10]{\Delta(f)/\Delta(g)}$ and factor n
So we spend hours factoring!

Global Reduction of $\Delta(f)$

If we know the prime factorisation of $\Delta(f)$, then the previous local algorithms gives a global algorithm.
Do we need to factorise? It seems essential:
Let p and q be large unknown primes, $n = p^2q$ and

$$f = n^2x^6 + x + 1$$

this has $\Delta(f) = (5^2 - 6^6n^2)n^8$
Let $g = f(x/p)p^2 = q^2x^6 + px + p^2$ with
$\Delta(g) = (5^5 - 6^6n^2)p^6q^8 = \Delta(f)/p^{10}$
For most p and q, g is the minimal model.
If we can compute g, then we can find $p = \sqrt[10]{\Delta(f)/\Delta(g)}$ and factor n
So we spend hours factoring!
Which we did not need to!

Limited Factoring

The overall goals given f and (not necessarily prime) number n is to:

- Make $\Delta(f)$ smaller at the primes dividing n without affecting other primes
- Find a non-trivial factor of n, **or**
- Prove that f is minimal at all primes dividing n

In theory we can't (e.g., we don't know how to factor $n = p^2 q$)

Limited Factoring

The overall goals given f and (not necessarily prime) number n is to:

- Make $\Delta(f)$ smaller at the primes dividing n without affecting other primes
- Find a non-trivial factor of n, **or**
- Prove that f is minimal at all primes dividing n

In theory we can't (e.g., we don't know how to factor $n = p^2 q$)
But in practise:

- We now trial division
- We can recognise pure powers
- If we pretend n is a prime:
  - Recall that $\gcd(\overline{f}, \overline{f}', \overline{f}'', \overline{f}''') = \sum a_i x^i \implies t = -a_{n-1}/(n a_n)$.
    So we can use Euclid's algorithm and division, either get $\overline{t}$ or a non-trivial factor of n
    If n is square-free, we can use $f(nx + t)/n^4$

Example

$p = 2$

$$\begin{aligned} f &= 34012224032614x^6 + 7725876689093409 0x^5 + 7312220374779630 5025x^4 \\ &\quad + 3691046351444189299100 0x^3 + 1048026473425102917957750 0x^2 \\ &\quad + 1587061422941652497077218750x + 1001391672848285343364330937 50 \end{aligned}$$

$$\Delta(f) = -2^{26} \cdot 3^{30}.$$

884803377138419832953641819894482509084594355194671943165046998557338268328551203012466430664062 5

Example

$p = 2$

$$\begin{aligned} f &= 34012224032614x^6 + 7725876689093409 0x^5 + 7312220374779630 5025x^4 \\ &\quad + 3691046351444189299100 0x^3 + 1048026473425102917957750 0x^2 \\ &\quad + 1587061422941652497077218750x + 1001391672848285343364330937 50 \end{aligned}$$

$$\Delta(f) = -2^{26} \cdot 3^{30} \cdot$$

$$8848033771384198329536418198944825090845943551946719431650469985573382683285512030124664306640625$$

$G := \gcd(I_2, I_4, I_6, I_{10}) = 2^9 \cdot 3^7 \cdot 1628299844445312 5$. Let us deal with 2

Example

$p = 2$

$$\begin{aligned} f &= 34012224032614x^6 + 7725876689093409 0x^5 + 731222037477963050 25x^4 \\ &+ 3691046351444189299100 0x^3 + 1048026473425102917957750 0x^2 \\ &+ 1587061422941652497077218750x + 1001391672848285343364330 93750 \end{aligned}$$

$$\Delta(f) = -2^{26} \cdot 3^{30} \cdot$$

$$8848033771384198329536418198944825090845943551946719431650469985573382683285512030124664306640625$$

$G := \gcd(I_2, I_4, I_6, I_{10}) = 2^9 \cdot 3^7 \cdot 1628299844445312 5$. Let us deal with 2

$f \mod 2 = x^4$. So we replace f by $f(2x)/2^4$.

Example

$p = 2$

$$\begin{aligned} f &= 34012224032614x^6 + 7725876689093409 0x^5 + 731222037477963050 25x^4 \\ &\quad + 3691046351444189299100 0x^3 + 1048026473425102917957750 0x^2 \\ &\quad + 1587061422941652497077218750x + 1001391672848285343364330937 50 \end{aligned}$$

$$\Delta(f) = -2^{26} \cdot 3^{30} \cdot$$

$$8848033771384198329536418198944825090845943551946719431650469985573382683285512030124664306640625$$

$G := \gcd(I_2, I_4, I_6, I_{10}) = 2^9 \cdot 3^7 \cdot 1628299844445312 5$. Let us deal with 2
$f \mod 2 = x^4$. So we replace f by $f(2x)/2^4$.

$$\begin{aligned} f &= 136048896130456x^6 + 1545175337818681 80x^5 + 731222037477963050 25x^4 \\ &\quad + 1845523175722094649550 0x^3 + 2620066183562757294894375x^2 \\ &\quad + 7935307114708262485386093 75/4x + 5006958364241426716821654 6875/8 \\ G &= 2^{11} \cdot 3^7 \cdot 1628299844445312 5 \end{aligned}$$

What went wrong?! Nothing, this just show that f is already minimal at 2.

Example

$p = 3$

$$
\begin{aligned}
f &= 34012224032614x^6 + 7725876689093409 0x^5 + 7312220374779630 5025x^4 \\
&\quad + 3691046351444189299100 0x^3 + 1048026473425102917957750 0x^2 \\
&\quad + 1587061422941652497077218750x + 1001391672848285343364330937 50 \\
G &= 2^9 \cdot 3^7 \cdot 1628299844445312 5
\end{aligned}
$$

Example

$p = 3$

$$
\begin{aligned}
f &= 34012224032614x^6 + 7725876689093409 0x^5 + 7312220374779630 5025x^4 \\
&\quad + 3691046351444189299100 0x^3 + 1048026473425102917957750 0x^2 \\
&\quad + 1587061422941652497077218750x + 1001391672848285343364330937 50 \\
G &= 2^9 \cdot 3^7 \cdot 1628299844445312 5
\end{aligned}
$$

$f \mod 3 = x^6 + x^3 + 1 = (x+2)^6$. So we replace f by $f(3x-1)/3^4$. This has integral coefficients

Example

$p = 3$

$$
\begin{aligned}
f &= 34012224032614x^6 + 7725876689093409 0x^5 + 7312220374779630 5025x^4 \\
&\quad + 3691046351444189299 1000x^3 + 1048026473425102917957 7500x^2 \\
&\quad + 1587061422941652497077218750x + 1001391672848285343364330 93750 \\
G &= 2^9 \cdot 3^7 \cdot 1628299844445 3125
\end{aligned}
$$

$f \mod 3 = x^6 + x^3 + 1 = (x+2)^6$. So we replace f by $f(3x-1)/3^4$.
This has integral coefficients
$f \mod 3 = 0$, so we replace f by $f/3$.
As $f \mod 3 = 0$ again, we replace f by $f/3$ once more.

Example

$p = 3$

$$
\begin{aligned}
f &= 34012224032614x^6 + 7725876689093409 0x^5 + 7312220374779630 5025x^4 \\
&\quad + 3691046351444189299 1000x^3 + 1048026473425102917957 7500x^2 \\
&\quad + 1587061422941652497077218750x + 1001391672848285343364330 93750 \\
G &= 2^9 \cdot 3^7 \cdot 1628299844445312 5
\end{aligned}
$$

$f \mod 3 = x^6 + x^3 + 1 = (x+2)^6$. So we replace f by $f(3x-1)/3^4$.
This has integral coefficients
$f \mod 3 = 0$, so we replace f by $f/3$.
As $f \mod 3 = 0$ again, we replace f by $f/3$ once more.

$$
\begin{aligned}
f &= 34012224032614x^6 + 2568489784891280 2x^5 + 8081824455189124865x^4 \\
&\quad + 1356249874328708757760x^3 + 1280243370969469719701 60x^2 \\
&\quad + 6445314126588347877869512x + 1352023995736661144304 14081 \\
G &= 2^9 \cdot 1628299844445312 5
\end{aligned}
$$

Example

$n = 1628299844445312 5$

This is not a perfect power, and let us pretend there is no obvious prime factors.

We work over $R = \mathbb{Z}/n\mathbb{Z}$, let $\overline{f} = f \mod n \in R[x]$

The degree of $\overline{f}$ is 6 (as $1628299844445312 5 \nmid 34012224032614$)

We compute $\gcd(f, \overline{f}')$ using Euclid's algorithm:

Find r_1 and q_1 such that $\overline{f} = q_1\overline{f}' + r_1$ (with r_1 having degree ≤ 4)

We find $r_1 = 1140308188054420 0x^4 + 12109289474605400x^3 + \ldots$

Example

$n = 1628299844445312 5$

This is not a perfect power, and let us pretend there is no obvious prime factors.

We work over $R = \mathbb{Z}/n\mathbb{Z}$, let $\overline{f} = f \mod n \in R[x]$

The degree of $\overline{f}$ is 6 (as $1628299844445312 5 \nmid 34012224032614$)

We compute $\gcd(f, \overline{f}')$ using Euclid's algorithm:

Find r_1 and q_1 such that $\overline{f} = q_1\overline{f}' + r_1$ (with r_1 having degree ≤ 4)

We find $r_1 = 1140308188054420 0x^4 + 12109289474605400x^3 + \ldots$

But: $\gcd(1140308188054420 0, 1628299844445312 5) = 148225 = (5 \cdot 77)^2$

Let us work with 5.

Example

$n = 1628299844445312 5$

This is not a perfect power, and let us pretend there is no obvious prime factors.

We work over $R = \mathbb{Z}/n\mathbb{Z}$, let $\overline{f} = f \mod n \in R[x]$

The degree of $\overline{f}$ is 6 (as $1628299844445312 5 \nmid 34012224032614$)

We compute $\gcd(f, \overline{f}')$ using Euclid's algorithm:

Find r_1 and q_1 such that $\overline{f} = q_1\overline{f}' + r_1$ (with r_1 having degree ≤ 4)

We find $r_1 = 1140308188054420 0x^4 + 1210928947460540 0x^3 + \ldots$

But: $\gcd(1140308188054420 0, 1628299844445312 5) = 148225 = (5 \cdot 77)^2$

Let us work with 5.

We find that $f \mod 5 = 4x^6 + 2x^5 + 2x + 1 = 4(x+3)^6$. As before:

$$\begin{aligned} f &= 34012224032614x^6 + 5014535563265150x^5 + 30804570550799342 9x^4 \\ &\quad + 1009249004057491040 0x^3 + 1859961810416028785 00x^2 \\ &\quad + 1828135797237179816690x + 7486893177107988656714 \\ G &= 2^9 \cdot 208422380089 \end{aligned}$$

Example

$n = 77$

We now work with $n = 208422380089$. But this is a perfect power: $208422380089 = 77^6$. Let us once more pretend that we do not know the factors of 77.

Example

$n = 77$

We now work with $n = 208422380089$. But this is a perfect power: $208422380089 = 77^6$. Let us once more pretend that we do not know the factors of 77.
We work over $R = \mathbb{Z}/77\mathbb{Z}$ and find that

$$\begin{aligned}
\overline{f} &= 58x^6 + 76x^5 + 53x^4 + 47x^3 + 15x^2 + 73x + 9 \\
\overline{f}' &= 40x^5 + 72x^4 + 58x^3 + 64x^2 + 30x + 73 \\
\overline{f}'' &= 46x^4 + 57x^3 + 20x^2 + 51x + 30 \\
\overline{f}''' &= 30x^3 + 17x^2 + 40x + 51
\end{aligned}$$

$\overline{f} = \overline{f}'(13x + 17), \overline{f}' = \overline{f}''(31x + 5)$ and $\overline{f}'' = \overline{f}'''(58x + 64)$. Hence $\gcd(\overline{f}, \overline{f}', \overline{f}'', \overline{f}''') = \overline{f}'''$.

Example

$n = 77$

We now work with $n = 208422380089$. But this is a perfect power: $208422380089 = 77^6$. Let us once more pretend that we do not know the factors of 77.
We work over $R = \mathbb{Z}/77\mathbb{Z}$ and find that

$$\begin{aligned}
\overline{f} &= 58x^6 + 76x^5 + 53x^4 + 47x^3 + 15x^2 + 73x + 9 \\
\overline{f}' &= 40x^5 + 72x^4 + 58x^3 + 64x^2 + 30x + 73 \\
\overline{f}'' &= 46x^4 + 57x^3 + 20x^2 + 51x + 30 \\
\overline{f}''' &= 30x^3 + 17x^2 + 40x + 51
\end{aligned}$$

$\overline{f} = \overline{f}'(13x + 17), \overline{f}' = \overline{f}''(31x + 5)$ and $\overline{f}'' = \overline{f}'''(58x + 64)$. Hence $\gcd(\overline{f}, \overline{f}', \overline{f}'', \overline{f}''') = \overline{f}'''$.
So let $t = -17/(30 \cdot 3) \in R$. This lifts to $t = 52 \in \mathbb{Z}$. Replace f by $f(77x + 52)/77^4$.

Example

Result

$$\begin{aligned} f &= 34012224032614x^6 + 202939603395334x^5 + 504530402887461x^4 \\ &\quad + 668969941608784x^3 + 498940081451716x^2 \\ &\quad + 198467276844858x + 32894113477186 \end{aligned}$$

$$\gcd(I_2, I_4, I_6, I_{10}) = 2^9$$

There are no more primes to remove, so $\Delta(f)$ is minimal.
In fact $\Delta(f) = -2^{26} \cdot 24155992513265764849$
(As everyone knows 24155992513265764849 is prime)

The coefficients are still large and horrible. We now play around with $\mathrm{GL}_2(\mathbb{Z}) \times \{\pm 1\}$ orbits.

As $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ only changes the sign of some of the coefficients we work with $\mathrm{SL}_2(\mathbb{Z})$.

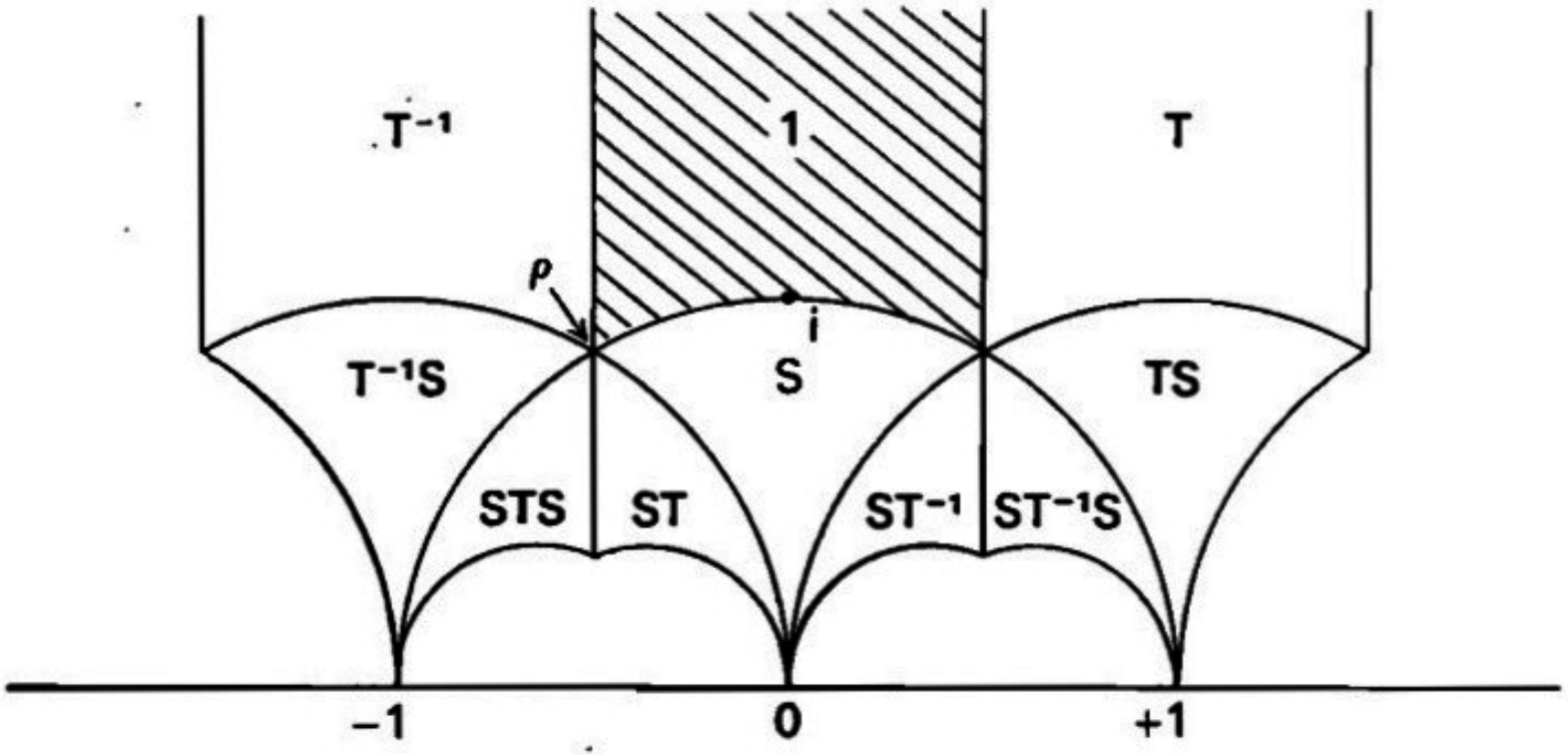
Idea: use a covariant $z = z(f) \in \mathcal{H} := \{z \in \mathbb{C} : \mathrm{im}(z) > 0\}$

z is such that

$$z(f \cdot A^{-1}) = A \cdot z = \frac{az + b}{cz + d} \quad \text{for all } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

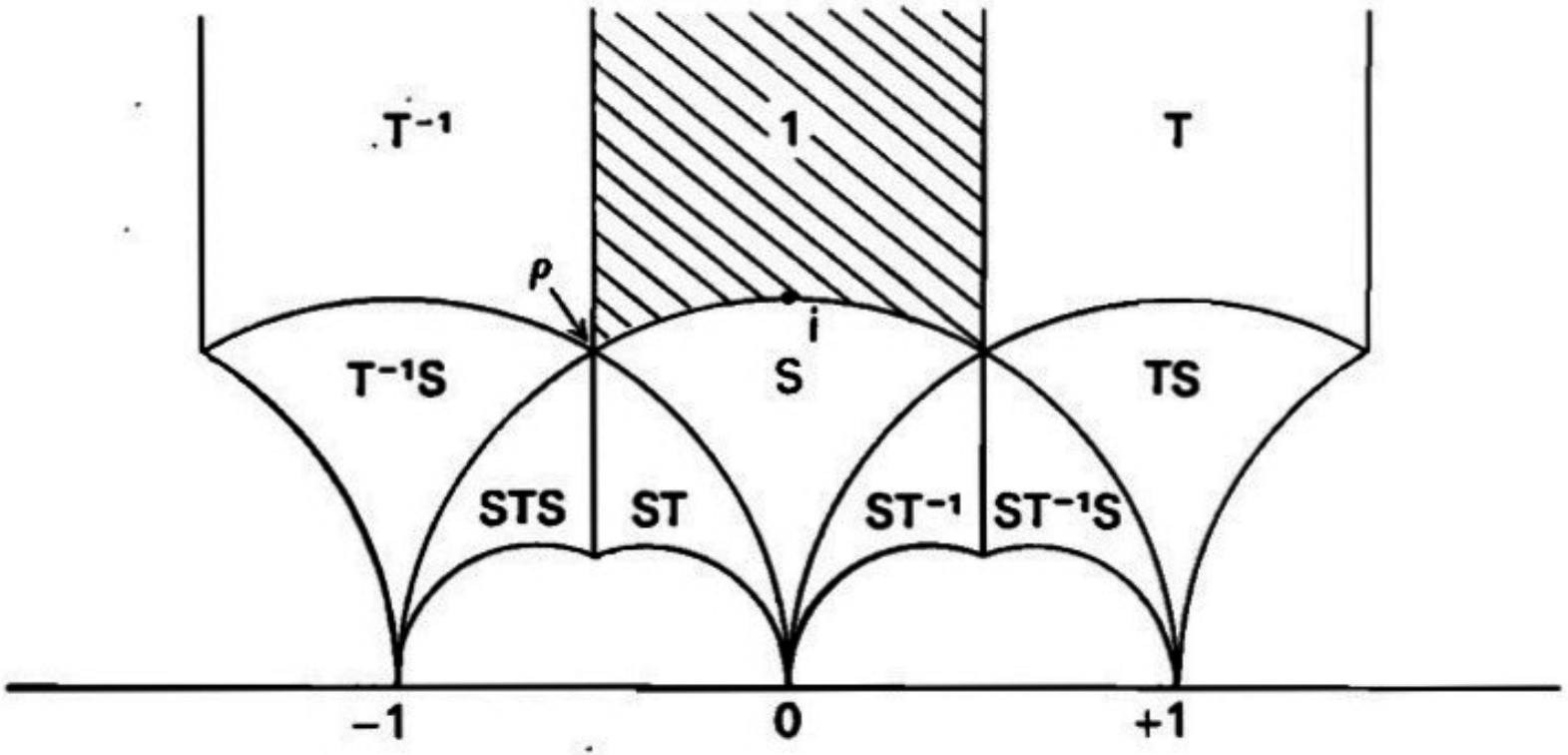
Stoll-Cremona Reduction

In $\mathcal{H}$ there is a fundamental domain that corresponds to $\mathrm{SL}_2(\mathbb{Z})$, namely $D = \{z = x + iy \in \mathcal{H} : |x| \leq 1/2, |z| > 1\}$



Stoll-Cremona Reduction

In $\mathcal{H}$ there is a fundamental domain that corresponds to $\mathrm{SL}_2(\mathbb{Z})$, namely $D = \{z = x + iy \in \mathcal{H} : |x| \leq 1/2, |z| > 1\}$



We say that f is *reduced* if and only if $z(f)$ is in the fundamental domain $\mathcal{D}$

What is z?

There are various covariants that one can use.

$z_0(f)$ is the root in $\mathcal{H}$ of

$$\sum_{j=1}^{6} |f'(\alpha_i)|^{-1/6} (x - \alpha_i)(x - \overline{\alpha_i})$$

(Easy to implement and fast to evaluate)

"*The representative point $z(F)$ is the unique point in upper half-space such that the sum of its distances from all the roots of F is minimal*".

[Prop 5.3 in Stoll-Cremona]

(This is natural and yields better reduction in practise)

What is z?

There are various covariants that one can use.

$z_0(f)$ is the root in $\mathcal{H}$ of

$$\sum_{j=1}^{6} |f'(\alpha_i)|^{-1/6} (x - \alpha_i)(x - \overline{\alpha_i})$$

(Easy to implement and fast to evaluate)

"*The representative point $z(F)$ is the unique point in upper half-space such that the sum of its distances from all the roots of F is minimal*".

[Prop 5.3 in Stoll-Cremona]

(This is natural and yields better reduction in practise)

Algorithm

Let $z = z(f)$

If $|z| < 1$, replace f by $f(-1/x)x^6$ (this replaces z with $-1/z$)

If $|x| > 1/2$, let m be the nearest integer to x, and replace f by $f(x + m)$ (this replaces z with $z - m$)

Repeat until $z \in \mathcal{D}$

Example

Stoll-Cremona Reduction

Recall that we had the equation

$$\begin{aligned} f &= 34012224032614x^6 + 202939603395334x^5 + 5045304028874 61x^4 \\ &\quad + 6689699416087 84x^3 + 498940081451716x^2 \\ &\quad + 19846727684485 8x + 328941134771 86 \\ z_0 &= -0.99444628675764 8 + 0.00010965005918218 0i \end{aligned}$$

Example

Stoll-Cremona Reduction

Recall that we had the equation

$$\begin{aligned} f &= 34012224032614x^6 + 202939603395334x^5 + 504530402887461x^4 \\ &\quad + 66896994160878 4x^3 + 498940081451716x^2 \\ &\quad + 198467276844858x + 32894113477186 \\ z_0 &= -0.99444628675764 8 + 0.000109650059182180i \end{aligned}$$

We apply the transformation $z_0 \mapsto z_0 + 1 \qquad f \mapsto f(x-1)$

Example

Stoll-Cremona Reduction

Recall that we had the equation

$$\begin{aligned} f &= 34012224032614x^6 + 202939603395334x^5 + 504530402887461x^4 \\ &\quad + 66896994160878 4x^3 + 49894008145171 6x^2 \\ &\quad + 19846727684485 8x + 32894113477186 \\ z_0 &= -0.99444628675764 8 + 0.00010965005918218 0i \end{aligned}$$

We apply the transformation $z_0 \mapsto z_0 + 1 \qquad f \mapsto f(x-1)$

$$\begin{aligned} f &= 34012224032614x^6 - 1133740800350x^5 + 15746400001x^4 \\ &\quad - 116640000x^3 + 486000x^2 - 1080x + 1 \\ z_0 &= 0.00555371324235188 + 0.00010965005918218 0i \end{aligned}$$

Example

Stoll-Cremona Reduction

We apply the transformation $z_0 \mapsto -1/z_0 \qquad f \mapsto f(-1/x)x^6$.

Example

Stoll-Cremona Reduction

We apply the transformation $z_0 \mapsto -1/z_0 \qquad f \mapsto f(-1/x)x^6$.

$$\begin{aligned} f &= x^6 + 1080x^5 + 486000x^4 + 116640000x^3 + 15746400001x^2 \\ &\quad + 1133740800350x + 34012224032614 \\ z_0 &= -179.989549368179 + 3.55363409653413i \end{aligned}$$

Example

Stoll-Cremona Reduction

We apply the transformation $z_0 \mapsto -1/z_0 \qquad f \mapsto f(-1/x)x^6$.

$$\begin{aligned} f &= x^6 + 1080x^5 + 486000x^4 + 116640000x^3 + 15746400001x^2 \\ &\quad + 1133740800350x + 34012224032614 \\ z_0 &= -179.989549368179 + 3.553634096534 13i \end{aligned}$$

We apply the transformation $z_0 \mapsto z_0 + 180 \qquad f \mapsto f(x - 180)$.

Example

Stoll-Cremona Reduction

We apply the transformation $z_0 \mapsto -1/z_0 \qquad f \mapsto f(-1/x)x^6$.

$$\begin{aligned} f &= x^6 + 1080x^5 + 486000x^4 + 116640000x^3 + 15746400001x^2 \\ &\quad + 1133740800350x + 34012224032614 \\ z_0 &= -179.989549368179 + 3.55363409653413i \end{aligned}$$

We apply the transformation $z_0 \mapsto z_0 + 180 \qquad f \mapsto f(x - 180)$.

$$\begin{aligned} f &= x^6 + x^2 - 10x + 2014 \\ z_0 &= 0.0104506318211433 + 3.55363409653413i \end{aligned}$$

Example

Stoll-Cremona Reduction

We apply the transformation $z_0 \mapsto -1/z_0 \qquad f \mapsto f(-1/x)x^6$.

$$\begin{aligned} f &= x^6 + 1080x^5 + 486000x^4 + 116640000x^3 + 15746400001x^2 \\ &\quad + 1133740800350x + 34012224032614 \\ z_0 &= -179.989549368179 + 3.55363409653413i \end{aligned}$$

We apply the transformation $z_0 \mapsto z_0 + 180 \qquad f \mapsto f(x - 180)$.

$$\begin{aligned} f &= x^6 + x^2 - 10x + 2014 \\ z_0 &= 0.0104506318211433 + 3.55363409653413i \end{aligned}$$

Now $z_0 \in \mathcal{D}$, so f is z_0-reduced

$z(f) = 0.010450538381635625239960129232 1 + 3.553635026337395813853516399 43i \in \mathcal{D}$

So f is also z-reduced. Note that $f(-x) = x^6 + x^2 + 10x + 2014$.

How to extend to a General Number Field

Let k be a number field

- Replace $\mathbb{Q}$ by k (and $\overline{\mathbb{Q}}$ by $\overline{k}$)
- Replace $\mathbb{Z}$ by $\mathcal{O}_k$ (the ring of integers)
- Replace the valuation v_p by by a place v and replace primes $p \in \mathbb{Z}$ by prime ideals of $\mathcal{O}_k$
- Replace the unit group $\{\pm 1\}$ by the unit group $\mathcal{O}_k^*$

Problems:

How to extend to a General Number Field

Let k be a number field

- Replace $\mathbb{Q}$ by k (and $\overline{\mathbb{Q}}$ by $\overline{k}$)
- Replace $\mathbb{Z}$ by $\mathcal{O}_k$ (the ring of integers)
- Replace the valuation v_p by by a place v and replace primes $p \in \mathbb{Z}$ by prime ideals of $\mathcal{O}_k$
- Replace the unit group $\{\pm 1\}$ by the unit group $\mathcal{O}_k^*$

Problems:

- What if k does not have class 1

- The fundamental domain of $\mathrm{SL}_2(\mathcal{O}_k)$ is not $\mathcal{D}$. The invariant z is also different.

How to extend to a General Number Field

Let k be a number field

- Replace $\mathbb{Q}$ by k (and $\overline{\mathbb{Q}}$ by $\overline{k}$)
- Replace $\mathbb{Z}$ by $\mathcal{O}_k$ (the ring of integers)
- Replace the valuation v_p by by a place v and replace primes $p \in \mathbb{Z}$ by prime ideals of $\mathcal{O}_k$
- Replace the unit group $\{\pm 1\}$ by the unit group $\mathcal{O}_k^*$

Problems:

- What if k does not have class 1
- We do not have a global minimality. But we can choose for it to be nearly minimal
- The fundamental domain of $\mathrm{SL}_2(\mathcal{O}_k)$ is not $\mathcal{D}$. The invariant z is also different.

How to extend to a General Number Field

Let k be a number field

- Replace $\mathbb{Q}$ by k (and $\overline{\mathbb{Q}}$ by $\overline{k}$)
- Replace $\mathbb{Z}$ by $\mathcal{O}_k$ (the ring of integers)
- Replace the valuation v_p by by a place v and replace primes $p \in \mathbb{Z}$ by prime ideals of $\mathcal{O}_k$
- Replace the unit group $\{\pm 1\}$ by the unit group $\mathcal{O}_k^*$

Problems:

- What if k does not have class 1
- We do not have a global minimality. But we can choose for it to be nearly minimal
- The fundamental domain of $\mathrm{SL}_2(\mathcal{O}_k)$ is not $\mathcal{D}$. The invariant z is also different.
- We had to extend the definition of the fundamental domain, and rewrite an algorithm to move the covariant z into the fundamental domain. We only did that for k being real quadratic of class number 1.

Our Results

We applied our algorithm to a database of hyperelliptic curves over number fields that contained the Igusa-Clebsch invariants but no model for the curve.

Thank you for your attention

Any questions?