Efficient resolution of Thue–Mahler equations

Adela Gherga

The University of Warwick

Background

A definition

- A *Thue–Mahler equation* is a Diophantine equation of the form

$$F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}$$

where

A definition

- A *Thue–Mahler equation* is a Diophantine equation of the form

$$F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}$$

where

- $F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_{d-1} X Y^{d-1} + a_d Y^d$

A definition

- A *Thue–Mahler equation* is a Diophantine equation of the form

$$F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}$$

  where

  - $F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_{d-1} X Y^{d-1} + a_d Y^d$
  - a is a fixed integer

A definition

- A *Thue–Mahler equation* is a Diophantine equation of the form

$$F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}$$

  where

  - $F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_{d-1} X Y^{d-1} + a_d Y^d$
  - a is a fixed integer
  - $p_1, \ldots, p_v$ are rational primes

A definition

- A *Thue–Mahler equation* is a Diophantine equation of the form

$$F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}$$

  where

  - $F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_{d-1} X Y^{d-1} + a_d Y^d$
  - a is a fixed integer
  - $p_1, \ldots, p_v$ are rational primes
  - $X, Y, z_1, \ldots, z_v$ are unknown integers

A definition

- A *Thue–Mahler equation* is a Diophantine equation of the form

$$F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}$$

  where

  - $F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_{d-1} X Y^{d-1} + a_d Y^d$
  - a is a fixed integer
  - $p_1, \ldots, p_v$ are rational primes
  - $X, Y, z_1, \ldots, z_v$ are unknown integers
  - $\gcd(X, Y) = 1$

Our main objective

Solve $F(X, Y) = a \cdot p_1^{z_1} \cdots p_v^{z_v}$

Why?

Why?

Theorem (Bennett, G., Rechnitzer)

Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N = 2^{\alpha}3^{\beta}N_0$ where N_0 is coprime to 6.

Then there exists an integral binary cubic form F of discriminant

$$D_F = sign(\Delta_E)2^{\alpha_0}3^{\beta_0}N_1,$$

and relatively prime integers u and v with

$$F(u,v) = c_0u^3 + c_1u^2v + c_2uv^2 + c_3v^3 = 2^{\alpha_1}3^{\beta_1}\prod_{p|N_0} p^{\kappa_p}$$

such that E is isomorphic over $\mathbb{Q}$ to $E_{\mathcal{D}}$, where

$$E_{\mathcal{D}} : 3^{[\beta_0/3]}y^2 = x^3 - 27\mathcal{D}^2H_F(u,v)x + 27\mathcal{D}^3G_F(u,v).$$

The algorithm

The algorithm

1. Compute all binary form F as given in the statement of the theorem

The algorithm

1. Compute all binary form F as given in the statement of the theorem
2. Solve the corresponding Thue–Mahler equations

The algorithm

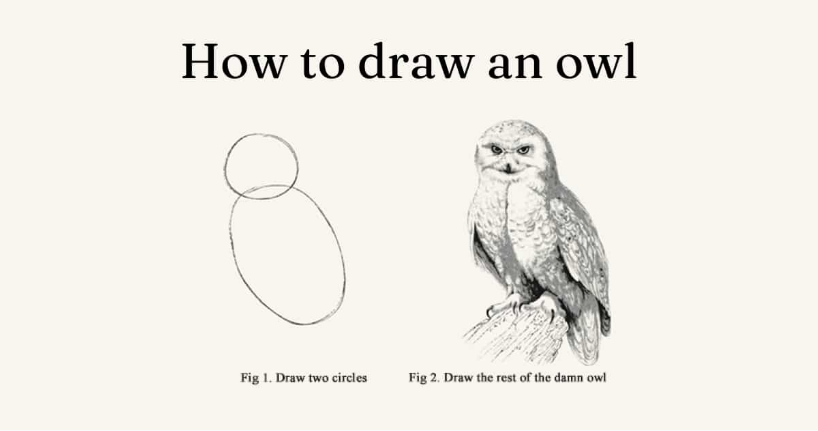
1. Compute all binary form F as given in the statement of the theorem
2. Solve the corresponding Thue–Mahler equations
3. Check “local” conditions and output the elliptic curves that arise

The algorithm

1. Compute all binary form F as given in the statement of the theorem
2. Solve the corresponding Thue–Mahler equations

An analogy

An analogy


How to draw an owl
Fig 1. Draw two circles
Fig 2. Draw the rest of the damn owl

A brief history

A brief history

- **Mahler (1933)**:
  A Thue–Mahler equation has at most finitely many solutions

A brief history

- **Mahler (1933)**:
  A Thue–Mahler equation has at most finitely many solutions
- **Sprindžuk, Vinogradov, Coates (1968/1969)**:
  An effective method exists to bound the number of solutions

A brief history

- **Mahler (1933)**:
  A Thue–Mahler equation has at most finitely many solutions
- **Sprindžuk, Vinogradov, Coates (1968/1969)**:
  An effective method exists to bound the number of solutions
- **Tzanakis, de Weger (1989)**:
  A practical method for solving the general Thue–Mahler equation

A brief history

- **Mahler (1933)**:
  A Thue–Mahler equation has at most finitely many solutions
- **Sprindžuk, Vinogradov, Coates (1968/1969)**:
  An effective method exists to bound the number of solutions
- **Tzanakis, de Weger (1989)**:
  A practical method for solving the general Thue–Mahler equation
- **Hambrook (2011)**:
  Implementation of a Thue–Mahler solver

Irreducible forms

For $N \leq 10^6$

Irreducible forms

For $N \leq 10^6$

- There are $6,078,277$ corresponding forms which need to be solved

Irreducible forms

For $N \leq 10^6$

- There are $6,078,277$ corresponding forms which need to be solved
- At 5 seconds per form, this requires 11.55 months on a single core

How bad could it be?

- A nice case
  $X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$

How bad could it be?

- A nice case
  $X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 4.1 minutes

How bad could it be?

- A nice case
  $X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 4.1 minutes
- A less nice case
  $3X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$

How bad could it be?

- A nice case
  $X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 4.1 minutes
- A less nice case
  $3X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 1.6 hours

How bad could it be?

- A nice case
  $X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 4.1 minutes
- A less nice case
  $3X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 1.6 hours
- A much less nice case
  $2X^3 + 20X^2Y - 14XY^2 + 37Y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 11^{z_4} \cdot 13^{z_5} \cdot 17^{z_6}$

How bad could it be?

- A nice case
  $X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 4.1 minutes
- A less nice case
  $3X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 1.6 hours
- A much less nice case
  $2X^3 + 20X^2Y - 14XY^2 + 37Y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 11^{z_4} \cdot 13^{z_5} \cdot 17^{z_6}$
  Total time: 4 hours

How bad could it be?

- A nice case
  $X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 4.1 minutes
- A less nice case
  $3X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 1.6 hours
- A much less nice case
  $2X^3 + 20X^2Y - 14XY^2 + 37Y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 11^{z_4} \cdot 13^{z_5} \cdot 17^{z_6}$
  Total time: 4 hours
- A really, really bad case
  $14X^3 + 20X^2Y + 24XY^2 + 15Y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}$

How bad could it be?

- A nice case
  $X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 4.1 minutes
- A less nice case
  $3X^3 + 3X^2Y + 44XY^2 + 66Y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$
  Total time: 1.6 hours
- A much less nice case
  $2X^3 + 20X^2Y - 14XY^2 + 37Y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 11^{z_4} \cdot 13^{z_5} \cdot 17^{z_6}$
  Total time: 4 hours
- A really, really bad case
  $14X^3 + 20X^2Y + 24XY^2 + 15Y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}$
  Total time: ????? months ☹

But wait, there's more!

But wait, there's more!

- Goormaghtigh's equation

But wait, there's more!

- Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}$$

But wait, there's more!

- Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^5 - 1}{y - 1}$$

But wait, there's more!

- Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^5 - 1}{y - 1} \implies \text{Thue–Mahler of degree 4}$$

But wait, there's more!

- Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^5 - 1}{y - 1} \implies \text{Thue–Mahler of degree 4}$$

$$189X^4 + 189X^3Y + 189X^2Y^2 + 189XY^3 + 190Y^4 = 2^{z_1} \cdot 5^{z_2} \cdot 19^{z_3}$$

But wait, there's more!

- Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^5 - 1}{y - 1} \implies \text{Thue–Mahler of degree 4}$$

$$189X^4 + 189X^3Y + 189X^2Y^2 + 189XY^3 + 190Y^4 = 2^{z_1} \cdot 5^{z_2} \cdot 19^{z_3}$$

Total time: 20 days

But wait, there's more!

- Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^5 - 1}{y - 1} \implies \text{Thue–Mahler of degree 4}$$

$$189X^4 + 189X^3Y + 189X^2Y^2 + 189XY^3 + 190Y^4 = 2^{z_1} \cdot 5^{z_2} \cdot 19^{z_3}$$

Total time: 20 days

- Ramanujan τ function

$$\tau(p^{m-1}) \neq \pm q^{z_1}$$

But wait, there's more!

- Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^5 - 1}{y - 1} \implies \text{Thue–Mahler of degree 4}$$

$$189X^4 + 189X^3Y + 189X^2Y^2 + 189XY^3 + 190Y^4 = 2^{z_1} \cdot 5^{z_2} \cdot 19^{z_3}$$

Total time: 20 days

- Ramanujan τ function

$$\tau(p^{m-1}) \neq \pm q^{z_1} \implies \text{Thue–Mahler of degree } \lfloor (m-1)/2 \rfloor$$

But wait, there's more!

- Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^5 - 1}{y - 1} \implies \text{Thue–Mahler of degree 4}$$

$$189X^4 + 189X^3Y + 189X^2Y^2 + 189XY^3 + 190Y^4 = 2^{z_1} \cdot 5^{z_2} \cdot 19^{z_3}$$

Total time: 20 days

- Ramanujan τ function

$$\tau(p^{m-1}) \neq \pm q^{z_1} \implies \text{Thue–Mahler of degree } \lfloor (m-1)/2 \rfloor$$

$$X^{20} - 210X^{19}Y + \cdots + 703X^2Y^{18} - 39XY^{19} + Y^{20} = \pm 83^{z_1}$$

But wait, there's more!

- Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^5 - 1}{y - 1} \implies \text{Thue–Mahler of degree 4}$$

$$189X^4 + 189X^3Y + 189X^2Y^2 + 189XY^3 + 190Y^4 = 2^{z_1} \cdot 5^{z_2} \cdot 19^{z_3}$$

Total time: 20 days

- Ramanujan τ function

$$\tau(p^{m-1}) \neq \pm q^{z_1} \implies \text{Thue–Mahler of degree } \lfloor (m-1)/2 \rfloor$$

$$X^{20} - 210X^{19}Y + \cdots + 703X^2Y^{18} - 39XY^{19} + Y^{20} = \pm 83^{z_1}$$

Total time: ????? months ☹

A new Thue–Mahler solver!

An example

Let

$$F(X, Y) = 3X^5 + 65X^4Y - 290X^3Y^2 - 2110X^2Y^3 + 975XY^4 + 3149Y^5.$$

Then $F(X, Y) = -2^5 \cdot 3^4 \cdot 5^{z_1} \cdot 11^{z_2}$ has no solutions

An example

Let

$$F(X,Y) = 3X^5 + 65X^4Y - 290X^3Y^2 - 2110X^2Y^3 + 975XY^4 + 3149Y^5.$$

Then $F(X,Y) \;=\; -2^5 \cdot 3^4 \cdot 5^{z_1} \cdot 11^{z_2}$ has no solutions

- Hambrook implementation of Tzanakis, de Weger: 72 days

An example

Let

$$F(X,Y) = 3X^5 + 65X^4Y - 290X^3Y^2 - 2110X^2Y^3 + 975XY^4 + 3149Y^5.$$

Then $F(X,Y) = -2^5 \cdot 3^4 \cdot 5^{z_1} \cdot 11^{z_2}$ has no solutions

- Hambrook implementation of Tzanakis, de Weger: 72 days
- Soydan, Tzanakis: 2.3 hours

An example

Let

$$F(X,Y) = 3X^5 + 65X^4Y - 290X^3Y^2 - 2110X^2Y^3 + 975XY^4 + 3149Y^5.$$

Then $F(X,Y) = -2^5 \cdot 3^4 \cdot 5^{z_1} \cdot 11^{z_2}$ has no solutions

- Hambrook implementation of Tzanakis, de Weger: 72 days
- Soydan, Tzanakis: 2.3 hours
- G., Siksek: 0.1 seconds ☺

An example

Let

$$F(X, Y) = 3X^5 + 65X^4Y - 290X^3Y^2 - 2110X^2Y^3 + 975XY^4 + 3149Y^5.$$

Then $F(X, Y) \ = \ -2^5 \cdot 3^4 \cdot 5^{z_1} \cdot 11^{z_2}$ has no solutions

- Hambrook implementation of Tzanakis, de Weger: 72 days
- Soydan, Tzanakis: 2.3 hours
- G., Siksek: 0.1 seconds ☺
  - $F(X, Y) = \pm\, 3^4 \cdot m$ has no solutions for $m \in \mathbb{Z}$, m coprime to 3

More examples

- $14X^3 + 20X^2Y + 24XY^2 + 15Y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}$

More examples

- $14X^3 + 20X^2Y + 24XY^2 + 15Y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}$
- $486X^{11} + 2673X^{10}Y + 8910X^9Y^2 + \cdots + 22XY^{10} + Y^{11} = 3^{z_1}$

Solving a Thue–Mahler equation

Overview

- Generate a very large upper bound for the solutions using the theory of linear forms in logarithms
- Reduce this bound via Diophantine approximation computations
- Search below this reduced bound

Setup

Initial steps

Given $F(X, Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d$

Initial steps

Given $F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d$

- Let $f(x) = a_0^{d-1} \cdot F(x/a_0, 1)$

Initial steps

Given $F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d$

- Let $f(x) = a_0^{d-1} \cdot F(x/a_0, 1)$
- Let $K = \mathbb{Q}(\theta)$ with $f(\theta) = 0$

Initial steps

Given $F(X,Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d$

- Let $f(x) = a_0^{d-1} \cdot F(x/a_0, 1)$
- Let $K = \mathbb{Q}(\theta)$ with $f(\theta) = 0$
- Solving $F(X,Y) = ap_1^{z_1} \cdots p_v^{z_v}$ is equivalent to solving

$$\mathrm{Norm}_{K/\mathbb{Q}}(a_0X - \theta Y) = a_0^{d-1} \cdot a \cdot p_1^{z_1} \cdots p_v^{z_v}$$

An equivalent problem

Given $\text{Norm}_{K/\mathbb{Q}}(a_0 X - \theta Y) = a_0^{d-1} \cdot a \cdot p_1^{z_1} \cdots p_v^{z_v}$

An equivalent problem

Given $\mathrm{Norm}_{K/\mathbb{Q}}(a_0X - \theta Y) = a_0^{d-1} \cdot a \cdot p_1^{z_1} \cdots p_v^{z_v}$

- There is a finite computable set of equations of the form

$$(a_0X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, \qquad S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$$

An equivalent problem

Given $\text{Norm}_{K/\mathbb{Q}}(a_0 X - \theta Y) = a_0^{d-1} \cdot a \cdot p_1^{z_1} \cdots p_v^{z_v}$

- There is a finite computable set of equations of the form

$$(a_0 X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, \qquad S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$$

  where

  - $\mathfrak{p}_i \in S$ is a prime ideal above p_i with $e(\mathfrak{p}_i)f(\mathfrak{p}_i) = 1$

An equivalent problem

Given $\text{Norm}_{K/\mathbb{Q}}(a_0X - \theta Y) = a_0^{d-1} \cdot a \cdot p_1^{z_1} \cdots p_v^{z_v}$

- There is a finite computable set of equations of the form

$$(a_0X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, \qquad S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$$

  where

  - $\mathfrak{p}_i \in S$ is a prime ideal above p_i with $e(\mathfrak{p}_i)f(\mathfrak{p}_i) = 1$
  - If $\mathfrak{p}_i$, $\mathfrak{p}_j \in S$ such that $\mathfrak{p}_i \mid p_i$ and $\mathfrak{p}_j \mid p_j$, then $p_i \neq p_j$

An equivalent problem

Given $\mathrm{Norm}_{K/\mathbb{Q}}(a_0 X - \theta Y) = a_0^{d-1} \cdot a \cdot p_1^{z_1} \cdots p_v^{z_v}$

- There is a finite computable set of equations of the form

$$(a_0 X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, \qquad S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$$

  where

  - $\mathfrak{p}_i \in S$ is a prime ideal above p_i with $e(\mathfrak{p}_i)f(\mathfrak{p}_i) = 1$
  - If $\mathfrak{p}_i, \mathfrak{p}_j \in S$ such that $\mathfrak{p}_i \mid p_i$ and $\mathfrak{p}_j \mid p_j$, then $p_i \neq p_j$
  - $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ of norm $|a_0^{d-1} \cdot a \cdot p_1^{t_1} \cdots p_v^{t_v}|$

An equivalent problem

Given $\mathrm{Norm}_{K/\mathbb{Q}}(a_0X - \theta Y) = a_0^{d-1} \cdot a \cdot p_1^{z_1} \cdots p_v^{z_v}$

- There is a finite computable set of equations of the form

$$(a_0X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, \qquad S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$$

  where

  - $\mathfrak{p}_i \in S$ is a prime ideal above p_i with $e(\mathfrak{p}_i)f(\mathfrak{p}_i) = 1$
  - If $\mathfrak{p}_i, \mathfrak{p}_j \in S$ such that $\mathfrak{p}_i \mid p_i$ and $\mathfrak{p}_j \mid p_j$, then $p_i \neq p_j$
  - $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ of norm $|a_0^{d-1} \cdot a \cdot p_1^{t_1} \cdots p_v^{t_v}|$

- Obtain a number of equations of the form

$$a_0X - Y\theta \ = \ \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad b_i \in \mathbb{Z},$$

  where $\delta_1, \ldots, \delta_r$ is a basis for $\mathcal{O}_S^\times/\text{torsion}$.

An example

$$5X^{11} + X^{10}Y + 4X^9Y^2 + X^8Y^3 + 6X^7Y^4 + X^6Y^5 + 6X^5Y^6 + \\ 6X^3Y^8 + 4XY^{10} - 2Y^{11} = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5}$$

An example

$$5X^{11} + X^{10}Y + 4X^9Y^2 + X^8Y^3 + 6X^7Y^4 + X^6Y^5 + 6X^5Y^6 + 6X^3Y^8 + 4XY^{10} - 2Y^{11} = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5}$$

- Two possiblities for $(5X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$

An example

$$5X^{11} + X^{10}Y + 4X^9Y^2 + X^8Y^3 + 6X^7Y^4 + X^6Y^5 + 6X^5Y^6 + 6X^3Y^8 + 4XY^{10} - 2Y^{11} = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5}$$

- Two possiblities for $(5X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$
- For one such ideal equation:

$$\mathfrak{p}_1 = \langle 11, 3+\theta \rangle, \quad \mathfrak{p}_2 = \langle 7, 1+\theta \rangle,$$
$$\mathfrak{p}_3 = \langle 5, \phi \rangle, \quad \mathfrak{p}_4 = \langle 3, 5+\theta \rangle, \quad \mathfrak{p}_5 = \langle 2, 1+\theta \rangle,$$

where

$$\phi = \frac{1}{5^9}(4\theta^{10} + 9\theta^9 + 185\theta^8 + 425\theta^7 + 4625\theta^6 + 13750\theta^5 + 131250\theta^4 + 750000\theta^3 + 3203125\theta^2 + 26953125\theta + 5859375)$$

An example - continued

- The corresponding equation $5X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}$ has

An example - continued

- The corresponding equation $5X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}$ has

$$\tau = \frac{1}{5^8}(11114\theta^{10} - 156626\theta^9 - 3960\theta^8 + 713050\theta^7 + 3733000\theta^6 - 1296637500\theta^5 + 175803125\theta^4$$
$$- 1846875000\theta^3 + 1457890625\theta^2 - 701687500000\theta + 134298828125)$$

$$\delta_1 = \frac{1}{5^9}(62639\theta^{10} - 748196\theta^9 - 4621980\theta^8 - 22207025\theta^7 + 38965000\theta^6 - 34195000\theta^5 - 449543750\theta^4$$
$$- 212713125000\theta^3 - 517657031250\theta^2 - 2098097656250\theta + 942912109375),$$

$$\delta_2 = \frac{1}{5^8}(-304507\theta^{10} - 1286200\theta^9 - 8286278\theta^8 - 147444530\theta^7 - 120138150\theta^6 + 2957350000\theta^5$$
$$+ 317693750\theta^4 + 196456718750\theta^3 - 1856078125\theta^2 + 1597415625000\theta - 1543269140625),$$

$$\delta_3 = \frac{1}{5^9}(-506181269733\theta^{10} - 151990813790480\theta^9 + 34170399960000\theta^8 + 206312637308500\theta^7$$
$$- 862101634598875\theta^6 - 112487612450893750\theta^5 + 132779534749000000\theta^4 - 479693441045625000\theta^3$$
$$- 481688292060625000\theta^2 - 552604241339570312500\theta + 1323149949666210937500),$$

$$\delta_4 = \frac{1}{5^9}(375938718\theta^{10} + 11130685130\theta^9 + 97012538300\theta^8 + 284204509000\theta^7 + 3376801042500\theta^6 + 8970753712500\theta^5$$
$$+ 88078172156250\theta^4 + 172701451406250\theta^3 + 2100841248437500\theta^2 + 4119271933593750\theta + 3744720025390625),$$

$$\vdots$$

$$\delta_{10} = \frac{1}{5^9}(-173\theta^{10} - 1528\theta^9 - 4840\theta^8 + 6800\theta^7 + 54125\theta^6 - 298750\theta^5 - 4609375\theta^4$$
$$- 195468750\theta^3 - 119531250\theta^2 + 2707031250\theta + 1181640625).$$

Height Bounds

Upper bounds

Given $a_0X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}$

Upper bounds

Given $a_0X - Y\theta \ = \ \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}$

- Let $B = \max\{|b_1|, \ldots, |b_r|\}$

Upper bounds

Given $a_0X - Y\theta \; = \; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}$

- Let $B = \max\{|b_1|, \ldots, |b_r|\}$
- Via linear forms in logarithms, we obtain

$$B \leq c_{20}$$

Upper bounds

Given $a_0 X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}$

- Let $B = \max\{|b_1|, \ldots, |b_r|\}$
- Via linear forms in logarithms, we obtain

$$B \leq c_{20}$$

- If $\mathbf{b} = (b_1, \ldots, b_r)$, let $\mathcal{B}_2$ denote the bound on the L^2-norm of $\mathbf{b}$

Upper bounds

Given $a_0X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}$

- Let $B = \max\{|b_1|, \ldots, |b_r|\}$
- Via linear forms in logarithms, we obtain

$$B \leq c_{20}$$

- If $\mathbf{b} = (b_1, \ldots, b_r)$, let $\mathcal{B}_2$ denote the bound on the L^2-norm of $\mathbf{b}$

$$\|\mathbf{b}\|_2 \leq \sqrt{r} \cdot c_{20} = \mathcal{B}_2$$

An example - continued

$$5X^{11} + X^{10}Y + 4X^9Y^2 + X^8Y^3 + 6X^7Y^4 + X^6Y^5 + 6X^5Y^6 + 6X^3Y^8 + 4XY^{10} - 2Y^{11} = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5}$$

An example - continued

$$5X^{11} + X^{10}Y + 4X^9Y^2 + X^8Y^3 + 6X^7Y^4 + X^6Y^5 + 6X^5Y^6 + 6X^3Y^8 + 4XY^{10} - 2Y^{11} = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5}$$

$$5X - \theta Y = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}, \qquad B = \max\{|b_1|, \dots, |b_{10}|\}$$

An example - continued

$$5X^{11} + X^{10}Y + 4X^9Y^2 + X^8Y^3 + 6X^7Y^4 + X^6Y^5 + 6X^5Y^6 + 6X^3Y^8 + 4XY^{10} - 2Y^{11} = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5}$$

$$5X - \theta Y = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}, \qquad B = \max\{|b_1|, \ldots, |b_{10}|\}$$

We obtain a bound of

$$B \leq 1.33 \times 10^{222} \implies \|\mathbf{b}\|_2 \leq 4.2 \times 10^{222}$$

Bound reduction

Bound reduction

$$a_0 X - Y\theta \;=\; \tau \cdot \underbrace{\delta_1^{b_1} \cdots \delta_r^{b_r}}_{\varepsilon}, \qquad B = \max\{|b_1|, \ldots, |b_r|\}$$

Bound reduction

$$a_0 X - Y\theta = \tau \cdot \underbrace{\delta_1^{b_1} \cdots \delta_r^{b_r}}_{\varepsilon}, \qquad B = \max\{|b_1|, \ldots, |b_r|\}$$

- Suppose $B \leq \mathcal{B}_0$

Bound reduction

$$a_0X - Y\theta \ = \ \tau \cdot \underbrace{\delta_1^{b_1} \cdots \delta_r^{b_r}}_{\varepsilon}, \qquad B = \max\{|b_1|, \ldots, |b_r|\}$$

- Suppose $B \leq \mathcal{B}_0$ (initially $\mathcal{B}_0 = c_{20}$)

Bound reduction

$$a_0 X - Y\theta \;=\; \tau \cdot \underbrace{\delta_1^{b_1} \cdots \delta_r^{b_r}}_{\varepsilon}, \qquad B = \max\{|b_1|, \ldots, |b_r|\}$$

- Suppose $B \leq \mathcal{B}_0$ (initially $\mathcal{B}_0 = c_{20}$)
- From initial bound computations,

$$B \leq 2c_{17} \sum_{\nu \in M_K} \log \max\{1, \|\varepsilon^{-1}\|_\nu\}$$

Bound reduction

$$a_0 X - Y\theta \;=\; \tau \cdot \underbrace{\delta_1^{b_1} \cdots \delta_r^{b_r}}_{\varepsilon}, \qquad B = \max\{|b_1|, \ldots, |b_r|\}$$

- Suppose $B \leq \mathcal{B}_0$ (initially $\mathcal{B}_0 = c_{20}$)
- From initial bound computations,

$$B \leq 2c_{17} \sum_{\nu \in M_K} \log \max\{1, \|\varepsilon^{-1}\|_\nu\}$$

- For all places $\nu \in M_K$, find ε_ν such that

$$B \leq \mathcal{B}_0 \implies \log \max\{1, \|\varepsilon^{-1}\|_\nu\} \leq \varepsilon_\nu$$

Bound reduction

$$a_0 X - Y\theta \ = \ \tau \cdot \underbrace{\delta_1^{b_1} \cdots \delta_r^{b_r}}_{\varepsilon}, \qquad B = \max\{|b_1|, \ldots, |b_r|\}$$

- Suppose $B \leq \mathcal{B}_0$ (initially $\mathcal{B}_0 = c_{20}$)
- From initial bound computations,

$$B \leq 2c_{17} \sum_{\nu \in M_K} \log \max\{1, \|\varepsilon^{-1}\|_\nu\}$$

- For all places $\nu \in M_K$, find ε_ν such that

$$B \leq \mathcal{B}_0 \implies \log \max\{1, \|\varepsilon^{-1}\|_\nu\} \leq \varepsilon_\nu$$

To find ε_ν:

Bound reduction

$$a_0X - Y\theta \; = \; \tau \cdot \underbrace{\delta_1^{b_1} \cdots \delta_r^{b_r}}_{\varepsilon}, \qquad B = \max\{|b_1|, \ldots, |b_r|\}$$

- Suppose $B \leq \mathcal{B}_0$ (initially $\mathcal{B}_0 = c_{20}$)
- From initial bound computations,

$$B \leq 2c_{17} \sum_{\nu \in M_K} \log \max\{1, \|\varepsilon^{-1}\|_\nu\}$$

- For all places $\nu \in M_K$, find ε_ν such that

$$B \leq \mathcal{B}_0 \implies \log \max\{1, \|\varepsilon^{-1}\|_\nu\} \leq \varepsilon_\nu$$

  To find ε_ν:

  - For $\nu = \mathfrak{p} \in S$, find k such that $\mathrm{ord}_\mathfrak{p}(a_0X - \theta Y) < k$

Bound reduction

$$a_0 X - Y\theta \;=\; \tau \cdot \underbrace{\delta_1^{b_1} \cdots \delta_r^{b_r}}_{\varepsilon}, \qquad B = \max\{|b_1|, \ldots, |b_r|\}$$

- Suppose $B \leq \mathcal{B}_0$ (initially $\mathcal{B}_0 = c_{20}$)
- From initial bound computations,

$$B \leq 2c_{17} \sum_{\nu \in M_K} \log \max\{1, \|\varepsilon^{-1}\|_\nu\}$$

- For all places $\nu \in M_K$, find ε_ν such that

$$B \leq \mathcal{B}_0 \implies \log \max\{1, \|\varepsilon^{-1}\|_\nu\} \leq \varepsilon_\nu$$

  To find ε_ν:

  - For $\nu = \mathfrak{p} \in S$, find k such that $\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y) < k$
  - For ν infinite, slightly annoying

Bound reduction

$$a_0X - Y\theta \;=\; \tau \cdot \underbrace{\delta_1^{b_1} \cdots \delta_r^{b_r}}_{\varepsilon}, \qquad B = \max\{|b_1|, \ldots, |b_r|\}$$

- Suppose $B \leq \mathcal{B}_0$ (initially $\mathcal{B}_0 = c_{20}$)
- From initial bound computations,

$$B \leq 2c_{17} \sum_{\nu \in M_K} \log \max\{1, \|\varepsilon^{-1}\|_\nu\}$$

- For all places $\nu \in M_K$, find ε_ν such that

$$B \leq \mathcal{B}_0 \implies \log \max\{1, \|\varepsilon^{-1}\|_\nu\} \leq \varepsilon_\nu$$

  To find ε_ν:

  - For $\nu = \mathfrak{p} \in S$, find k such that $\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y) < k$
  - For ν infinite, slightly annoying

- Obtain a new bound for B:

$$B \leq 2c_{17} \sum_{\nu \in M_K} \varepsilon_\nu \qquad \implies \text{ iterate!}$$

Valuations of $a_0X - \theta Y$

- Let $\mathfrak{p} \in S$ and $k \in \mathbb{Z}_{\geq 1}$

Valuations of $a_0 X - \theta Y$

- Let $\mathfrak{p} \in S$ and $k \in \mathbb{Z}_{\geq 1}$
- Suppose

$$\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y) \geq k \quad \Longrightarrow \; a_0 X - \theta Y \equiv 0 \pmod{\mathfrak{p}^k}$$

Valuations of $a_0 X - \theta Y$

- Let $\mathfrak{p} \in S$ and $k \in \mathbb{Z}_{\geq 1}$
- Suppose

$$\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y) \geq k \quad \implies a_0 X - \theta Y \equiv 0 \pmod{\mathfrak{p}^k}$$

- There is some $\theta_0 \in \mathbb{Z}$ such that $\theta - \theta_0 \equiv 0 \pmod{\mathfrak{p}^k}$

Valuations of $a_0 X - \theta Y$

- Let $\mathfrak{p} \in S$ and $k \in \mathbb{Z}_{\geq 1}$
- Suppose

$$\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y) \geq k \quad \implies a_0 X - \theta Y \equiv 0 \pmod{\mathfrak{p}^k}$$

- There is some $\theta_0 \in \mathbb{Z}$ such that $\theta - \theta_0 \equiv 0 \pmod{\mathfrak{p}^k}$

$$a_0 X - \theta_0 Y \equiv 0 \pmod{\mathfrak{p}^k}$$

Valuations of $a_0X - \theta Y$

- Let $\mathfrak{p} \in S$ and $k \in \mathbb{Z}_{\geq 1}$
- Suppose

$$\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y) \geq k \implies a_0X - \theta Y \equiv 0 \pmod{\mathfrak{p}^k}$$

- There is some $\theta_0 \in \mathbb{Z}$ such that $\theta - \theta_0 \equiv 0 \pmod{\mathfrak{p}^k}$

$$a_0X - \theta_0 Y \equiv 0 \pmod{\mathfrak{p}^k} \implies a_0X - \theta_0 Y \equiv 0 \pmod{p^k}$$

Valuations of $a_0 X - \theta Y$

- Let $\mathfrak{p} \in S$ and $k \in \mathbb{Z}_{\geq 1}$
- Suppose

$$\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y) \geq k \quad \implies a_0 X - \theta Y \equiv 0 \pmod{\mathfrak{p}^k}$$

- There is some $\theta_0 \in \mathbb{Z}$ such that $\theta - \theta_0 \equiv 0 \pmod{\mathfrak{p}^k}$

$$a_0 X - \theta_0 Y \equiv 0 \pmod{\mathfrak{p}^k} \quad \implies a_0 X - \theta_0 Y \equiv 0 \pmod{p^k}$$

- Recall $a_0 X - \theta Y = \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}$

Valuations of $a_0 X - \theta Y$

- Let $\mathfrak{p} \in S$ and $k \in \mathbb{Z}_{\geq 1}$
- Suppose

$$\mathrm{ord}_{\mathfrak{p}}(a_0 X - \theta Y) \geq k \quad \Longrightarrow a_0 X - \theta Y \equiv 0 \pmod{\mathfrak{p}^k}$$

- There is some $\theta_0 \in \mathbb{Z}$ such that $\theta - \theta_0 \equiv 0 \pmod{\mathfrak{p}^k}$

$$a_0 X - \theta_0 Y \equiv 0 \pmod{\mathfrak{p}^k} \quad \Longrightarrow a_0 X - \theta_0 Y \equiv 0 \pmod{p^k}$$

- Recall $a_0 X - \theta Y = \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv (a_0 X - \theta Y) - (a_0 X - \theta_0 Y) = Y(\theta_0 - \theta) \pmod{(p\mathcal{O}_K)^k}$$

Valuations of $a_0X - \theta Y$

- Let $\mathfrak{p} \in S$ and $k \in \mathbb{Z}_{\geq 1}$
- Suppose

$$\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y) \geq k \quad \Longrightarrow a_0X - \theta Y \equiv 0 \pmod{\mathfrak{p}^k}$$

- There is some $\theta_0 \in \mathbb{Z}$ such that $\theta - \theta_0 \equiv 0 \pmod{\mathfrak{p}^k}$

$$a_0X - \theta_0 Y \equiv 0 \pmod{\mathfrak{p}^k} \quad \Longrightarrow a_0X - \theta_0 Y \equiv 0 \pmod{p^k}$$

- Recall $a_0X - \theta Y = \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv (a_0X - \theta Y) - (a_0X - \theta_0 Y) = Y(\theta_0 - \theta) \pmod{(p\mathcal{O}_K)^k}$$

- Let $\mathfrak{a} = (p\mathcal{O}_K)/\mathfrak{p}$, then

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv Y(\theta_0 - \theta) \pmod{\mathfrak{a}^k}$$

Valuations of $a_0 X - \theta Y$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv Y(\theta_0 - \theta) \pmod{\mathfrak{a}^k}, \qquad \mathfrak{a} = (p\mathcal{O}_K)/\mathfrak{p}$$

Valuations of $a_0X - \theta Y$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv Y(\theta_0 - \theta) \pmod{\mathfrak{a}^k}, \qquad \mathfrak{a} = (p\mathcal{O}_K)/\mathfrak{p}$$

- Let $\phi : \mathbb{Z}^r \to (\mathcal{O}_K/\mathfrak{a}^k)^\times/(\mathbb{Z}/p^k\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$

Valuations of $a_0X - \theta Y$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv Y(\theta_0 - \theta) \pmod{\mathfrak{a}^k}, \qquad \mathfrak{a} = (p\mathcal{O}_K)/\mathfrak{p}$$

- Let $\phi : \mathbb{Z}^r \to (\mathcal{O}_K/\mathfrak{a}^k)^\times/(\mathbb{Z}/p^k\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$
- If $\mathbf{b} = (b_1, \ldots, b_r)$, then $\phi(\mathbf{b}) = \frac{\theta_0 - \theta}{\tau}$

Valuations of $a_0X - \theta Y$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv Y(\theta_0 - \theta) \pmod{\mathfrak{a}^k}, \qquad \mathfrak{a} = (p\mathcal{O}_K)/\mathfrak{p}$$

- Let $\phi : \mathbb{Z}^r \to (\mathcal{O}_K/\mathfrak{a}^k)^\times/(\mathbb{Z}/p^k\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$
- If $\mathbf{b} = (b_1, \ldots, b_r)$, then $\phi(\mathbf{b}) = \frac{\theta_0 - \theta}{\tau}$
- Contradiction if $\frac{\theta_0 - \theta}{\tau} \notin \text{Image}(\phi)$

Valuations of $a_0 X - \theta Y$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv Y(\theta_0 - \theta) \pmod{\mathfrak{a}^k}, \qquad \mathfrak{a} = (p\mathcal{O}_K)/\mathfrak{p}$$

- Let $\phi : \mathbb{Z}^r \to (\mathcal{O}_K/\mathfrak{a}^k)^\times/(\mathbb{Z}/p^k\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$
- If $\mathbf{b} = (b_1, \ldots, b_r)$, then $\phi(\mathbf{b}) = \frac{\theta_0 - \theta}{\tau}$
- Contradiction if $\frac{\theta_0 - \theta}{\tau} \notin \mathrm{Image}(\phi)$
- Thus suppose, for some $\mathbf{w} \in \mathbb{Z}^r$,

$$\phi(\mathbf{w}) = \frac{\theta_0 - \theta}{\tau}$$

Valuations of $a_0 X - \theta Y$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv Y(\theta_0 - \theta) \pmod{\mathfrak{a}^k}, \qquad \mathfrak{a} = (p\mathcal{O}_K)/\mathfrak{p}$$

- Let $\phi : \mathbb{Z}^r \to (\mathcal{O}_K/\mathfrak{a}^k)^\times/(\mathbb{Z}/p^k\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$
- If $\mathbf{b} = (b_1, \ldots, b_r)$, then $\phi(\mathbf{b}) = \frac{\theta_0 - \theta}{\tau}$
- Contradiction if $\frac{\theta_0 - \theta}{\tau} \notin \mathrm{Image}(\phi)$
- Thus suppose, for some $\mathbf{w} \in \mathbb{Z}^r$,

$$\phi(\mathbf{w}) = \frac{\theta_0 - \theta}{\tau} \implies \mathbf{b} \in \mathbf{w} + L, \quad L = \mathrm{Ker}(\phi)$$

Valuations of $a_0X - \theta Y$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv Y(\theta_0 - \theta) \pmod{\mathfrak{a}^k}, \qquad \mathfrak{a} = (p\mathcal{O}_K)/\mathfrak{p}$$

- Let $\phi : \mathbb{Z}^r \to (\mathcal{O}_K/\mathfrak{a}^k)^\times/(\mathbb{Z}/p^k\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$
- If $\mathbf{b} = (b_1, \ldots, b_r)$, then $\phi(\mathbf{b}) = \frac{\theta_0 - \theta}{\tau}$
- Contradiction if $\frac{\theta_0 - \theta}{\tau} \notin \text{Image}(\phi)$
- Thus suppose, for some $\mathbf{w} \in \mathbb{Z}^r$,

$$\phi(\mathbf{w}) = \frac{\theta_0 - \theta}{\tau} \implies \mathbf{b} \in \mathbf{w} + L, \quad L = \text{Ker}(\phi)$$

- Recall $\|\mathbf{b}\|_2 \leq \mathcal{B}_2$

Valuations of $a_0X - \theta Y$

$$\tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r} \equiv Y(\theta_0 - \theta) \pmod{\mathfrak{a}^k}, \qquad \mathfrak{a} = (p\mathcal{O}_K)/\mathfrak{p}$$

- Let $\phi : \mathbb{Z}^r \to (\mathcal{O}_K/\mathfrak{a}^k)^\times/(\mathbb{Z}/p^k\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$
- If $\mathbf{b} = (b_1, \ldots, b_r)$, then $\phi(\mathbf{b}) = \frac{\theta_0 - \theta}{\tau}$
- Contradiction if $\frac{\theta_0 - \theta}{\tau} \notin \mathrm{Image}(\phi)$
- Thus suppose, for some $\mathbf{w} \in \mathbb{Z}^r$,

$$\phi(\mathbf{w}) = \frac{\theta_0 - \theta}{\tau} \implies \mathbf{b} \in \mathbf{w} + L, \quad L = \mathrm{Ker}(\phi)$$

- Recall $\|\mathbf{b}\|_2 \le \mathcal{B}_2$

If $\mathbf{w} + L$ does not contain any vectors $\mathbf{v}$ with $\|\mathbf{v}\|_2 \le \mathcal{B}_2$, then

$$\mathrm{ord}_{\mathfrak{p}}(a_0X - \theta Y) \le k - 1$$

An example - continued

For $(5X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_5^{n_5}$, where $5X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}$:

An example - continued

For $(5X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_5^{n_5}$, where $5X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}$:

Iteration	$\mathcal{B}_0$	Bounds for $\text{ord}_{\mathfrak{p}_j}(5X - \theta Y)$ with $1 \leq j \leq 5$				
0	1.33×10^{222}	237	292	355	518	821

An example - continued

For $(5X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_5^{n_5}$, where $5X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}$:

Iteration	$\mathcal{B}_0$	Bounds for $\mathrm{ord}_{\mathfrak{p}_j}(5X - \theta Y)$ with $1 \leq j \leq 5$				
0	1.33×10^{222}	237	292	355	518	821
1	8285	4	5	7	10	15

An example - continued

For $(5X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_5^{n_5}$, where $5X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}$:

Iteration	$\mathcal{B}_0$	Bounds for $\mathrm{ord}_{\mathfrak{p}_j}(5X - \theta Y)$ with $1 \leq j \leq 5$				
0	1.33×10^{222}	237	292	355	518	821
1	8285	4	5	7	10	15
2	236	2	3	5	6	10

An example - continued

For $(5X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_5^{n_5}$, where $5X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}$:

Iteration	$\mathcal{B}_0$	Bounds for $\text{ord}_{\mathfrak{p}_j}(5X - \theta Y)$ with $1 \leq j \leq 5$				
0	1.33×10^{222}	237	292	355	518	821
1	8285	4	5	7	10	15
2	236	2	3	5	6	10
3	179	2	3	5	6	9

An example - continued

For $(5X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_5^{n_5}$, where $5X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}$:

Iteration	$\mathcal{B}_0$	Bounds for $\mathrm{ord}_{\mathfrak{p}_j}(5X - \theta Y)$ with $1 \leq j \leq 5$				
0	1.33×10^{222}	237	292	355	518	821
1	8285	4	5	7	10	15
2	236	2	3	5	6	10
3	179	2	3	5	6	9
4	179	2	3	5	6	9

An example - continued

For $(5X - \theta Y)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_5^{n_5}$, where $5X - Y\theta = \tau \cdot \delta_1^{b_1} \cdots \delta_{10}^{b_{10}}$:

Iteration	$\mathcal{B}_0$	Bounds for $\mathrm{ord}_{\mathfrak{p}_j}(5X - \theta Y)$ with $1 \leq j \leq 5$				
0	1.33×10^{222}	237	292	355	518	821
1	8285	4	5	7	10	15
2	236	2	3	5	6	10
3	179	2	3	5	6	9
4	179	2	3	5	6	9

$$B = \max\{|b_1|, \ldots, |b_{10}|\} \leq 179 \implies \|\mathbf{b}\|_2 \leq 567$$

Searching below the reduced bound

Sieving

$$a_0 X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \leq \mathcal{B}_2$$

Sieving

$$a_0X - Y\theta \; = \; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \leq \mathcal{B}_2$$

- Let q be a prime coprime to the support of τ, $\delta_1, \ldots, \delta_r$

Sieving

$$a_0X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \leq \mathcal{B}_2$$

- Let q be a prime coprime to the support of τ, $\delta_1, \ldots, \delta_r$
- Let $\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi_q(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$

Sieving

$$a_0 X - Y\theta \ = \ \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \leq \mathcal{B}_2$$

- Let q be a prime coprime to the support of τ, $\delta_1, \ldots, \delta_r$
- Let $\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi_q(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$
- Then $\phi_q(\mathbf{b}) \in R_q$, where

$$R_q := \left\{ \frac{a_0 u - \theta}{\tau} \ : \ u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\} \subset (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times$$

Sieving

$$a_0X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \le \mathcal{B}_2$$

- Let q be a prime coprime to the support of τ, $\delta_1, \ldots, \delta_r$
- Let $\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi_q(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$
- Then $\phi_q(\mathbf{b}) \in R_q$, where

$$R_q := \left\{ \frac{a_0 u - \theta}{\tau} \;:\; u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\} \subset (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times$$

  - If $q \mid Y$, then $\phi_q(\mathbf{b}) = \delta_1^{b_1} \cdots \delta_r^{b_r} = (a_0X - \theta Y)/\tau = a_0/\tau$

Sieving

$$a_0X - Y\theta \ = \ \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \leq \mathcal{B}_2$$

- Let q be a prime coprime to the support of τ, $\delta_1, \ldots, \delta_r$
- Let $\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi_q(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$
- Then $\phi_q(\mathbf{b}) \in R_q$, where

$$R_q := \left\{ \frac{a_0 u - \theta}{\tau} \ : \ u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\} \subset (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times$$

- If $q \mid Y$, then $\phi_q(\mathbf{b}) = \delta_1^{b_1} \cdots \delta_r^{b_r} = (a_0X - \theta Y)/\tau = a_0/\tau$
- If $q \nmid Y$, then $\phi_q(\mathbf{b}) = \delta_1^{b_1} \cdots \delta_r^{b_r} = (a_0X - \theta Y)/\tau = (a_0X/Y - \theta)/\tau$

Sieving

$$a_0 X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \leq \mathcal{B}_2$$

Sieving

$$a_0 X - Y\theta \; = \; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \le \mathcal{B}_2$$

$$\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$$

Sieving

$$a_0 X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \le \mathcal{B}_2$$

$$\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$$

$$\phi_q(\mathbf{b}) \in R_q = \left\{ \frac{a_0 u - \theta}{\tau} \;:\; u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\}$$

Sieving

$$a_0 X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \le \mathcal{B}_2$$

$$\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$$

$$\phi_q(\mathbf{b}) \in R_q = \left\{ \frac{a_0 u - \theta}{\tau} \;:\; u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\}$$

- Let $L_q = \ker(\phi_q) \subset \mathbb{Z}^r$

Sieving

$$a_0X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \leq \mathcal{B}_2$$

$$\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$$

$$\phi_q(\mathbf{b}) \in R_q = \left\{ \frac{a_0 u - \theta}{\tau} \;:\; u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\}$$

- Let $L_q = \ker(\phi_q) \subset \mathbb{Z}^r$
- Let W_q be a set of preimages under ϕ_q of elements of R_q

Sieving

$$a_0 X - Y\theta \; = \; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \leq \mathcal{B}_2$$

$$\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K / q\mathcal{O}_K)^\times / (\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$$

$$\phi_q(\mathbf{b}) \in R_q = \left\{ \frac{a_0 u - \theta}{\tau} \; : \; u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\}$$

- Let $L_q = \ker(\phi_q) \subset \mathbb{Z}^r$
- Let W_q be a set of preimages under ϕ_q of elements of R_q
- Thus $\mathbf{b} \in W_q + L_q$

Sieving

$$a_0X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \leq \mathcal{B}_2$$

$$\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi(x_1, \ldots, x_r) = \delta_1^{x_1} \cdots \delta_r^{x_r}$$

$$\phi_q(\mathbf{b}) \in R_q = \left\{ \frac{a_0 u - \theta}{\tau} \;:\; u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\}$$

- Let $L_q = \ker(\phi_q) \subset \mathbb{Z}^r$
- Let W_q be a set of preimages under ϕ_q of elements of R_q
- Thus $\mathbf{b} \in W_q + L_q$

Choose several primes $q_1, \ldots, q_n$.

Sieving

$$a_0 X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \le \mathcal{B}_2$$

$$\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi(x_1,\dots,x_r) = \delta_1^{x_1}\cdots\delta_r^{x_r}$$

$$\phi_q(\mathbf{b}) \in R_q = \left\{ \frac{a_0 u - \theta}{\tau} \;:\; u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\}$$

- Let $L_q = \ker(\phi_q) \subset \mathbb{Z}^r$
- Let W_q be a set of preimages under ϕ_q of elements of R_q
- Thus $\mathbf{b} \in W_q + L_q$

Choose several primes $q_1, \dots, q_n$. Then

$$\mathbf{b} \;\in\; \bigcap_{i=1}^{n} (W_{q_i} + L_{q_i}) \;=\; W + L, \qquad L = \bigcap L_{q_i}$$

Sieving

$$a_0 X - Y\theta \;=\; \tau \cdot \delta_1^{b_1} \cdots \delta_r^{b_r}, \qquad \|\mathbf{b}\|_2 \le \mathcal{B}_2$$

$$\phi_q : \mathbb{Z}^r \to (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times, \quad \phi(x_1,\dots,x_r) = \delta_1^{x_1}\cdots\delta_r^{x_r}$$

$$\phi_q(\mathbf{b}) \in R_q = \left\{ \frac{a_0 u - \theta}{\tau} \;:\; u \in \mathbb{F}_q \right\} \cup \left\{ \frac{a_0}{\tau} \right\}$$

- Let $L_q = \ker(\phi_q) \subset \mathbb{Z}^r$
- Let W_q be a set of preimages under ϕ_q of elements of R_q
- Thus $\mathbf{b} \in W_q + L_q$

Choose several primes $q_1, \dots, q_n$. Then

$$\mathbf{b} \;\in\; \bigcap_{i=1}^{n} (W_{q_i} + L_{q_i}) \;=\; W + L, \qquad L = \bigcap L_{q_i}$$

L has huge index $\implies$ easy to determine $\mathbf{b}$ using Finke and Pohst!

Examples

An appeal to your generosity

An appeal to your generosity

Looking for donations

An appeal to your generosity

Looking for donations: Cores with Magma and storage!

An appeal to your generosity

Looking for donations: Cores with Magma and storage!

$\Longrightarrow$ adela.gherga@warwick.ac.uk

Thank You