

Computing elliptic curves over \mathbb{Q} via Thue-Mahler equations, and related problems

Adela Gherga

The University of British Columbia

Thue-Mahler equations

- Let $S = \{p_1, \dots, p_v\}$ be a set of prime numbers

- Let $S = \{p_1, \dots, p_v\}$ be a set of prime numbers
- A *Thue-Mahler equation* is a Diophantine equations of the form

$$F(x, y) = ap_1^{z_1} \cdots p_v^{z_v}$$

where

- Let $S = \{p_1, \dots, p_v\}$ be a set of prime numbers
- A *Thue-Mahler equation* is a Diophantine equations of the form

$$F(x, y) = ap_1^{z_1} \cdots p_v^{z_v}$$

where

- $F(x, y) = c_0x^n + c_1x^{n-1}y + \cdots + c_{n-1}xy^{n-1} + c_ny^n$

- Let $S = \{p_1, \dots, p_v\}$ be a set of prime numbers
- A *Thue-Mahler equation* is a Diophantine equations of the form

$$F(x, y) = ap_1^{z_1} \cdots p_v^{z_v}$$

where

- $F(x, y) = c_0x^n + c_1x^{n-1}y + \cdots + c_{n-1}xy^{n-1} + c_ny^n$
- a is a fixed integer

- Let $S = \{p_1, \dots, p_v\}$ be a set of prime numbers
- A *Thue-Mahler equation* is a Diophantine equations of the form

$$F(x, y) = ap_1^{z_1} \cdots p_v^{z_v}$$

where

- $F(x, y) = c_0x^n + c_1x^{n-1}y + \cdots + c_{n-1}xy^{n-1} + c_ny^n$
- a is a fixed integer
- x, y, z_1, \dots, z_v are unknown integers

Given S, F and a , find all solutions (x, y, z_1, \dots, z_v) satisfying

$$F(x, y) = ap_1^{z_1} \cdots p_v^{z_v}$$

Why?

Why?

- Compute elliptic curves

Why?

- Compute elliptic curves
- Solve other Diophantine equations

Why?

- Compute elliptic curves
- Solve other Diophantine equations
- At least 4 people heard about this project and emailed me asking for solutions to very specific Thue-Mahler equations

Is this even possible?

Is this even possible?

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

Is this even possible?

- **Mahler (1933):** A Thue-Mahler equation has at most finitely many solutions
 - This argument is ineffective

Is this even possible?

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

Is this even possible?

- **Mahler (1933)**: A Thue-Mahler equation has at most finitely many solutions
 - This argument is ineffective
- **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

Is this even possible?

- **Mahler (1933)**: A Thue-Mahler equation has at most finitely many solutions
 - This argument is ineffective
- **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

Why?

- Compute elliptic curves
- Solve other Diophantine equations
- At least 4 people heard about this project and emailed me asking for solutions to very specific Thue-Mahler equations

Why?

- Compute elliptic curves

Elliptic Curves

- An *elliptic curve* is a nonsingular curve defined by

$$E : y^2 = x^3 + ax + b$$

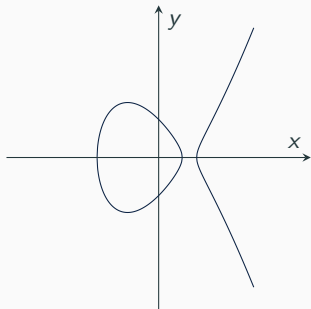
- An *elliptic curve* is a nonsingular curve defined by

$$E : y^2 = x^3 + ax + b$$

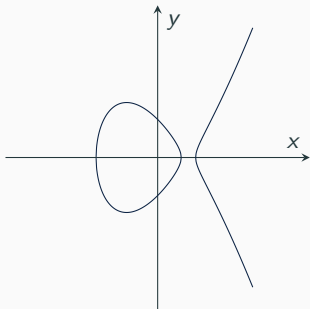
- A curve is nonsingular $\iff \Delta_E = 4a^3 + 27b^2 \neq 0$.



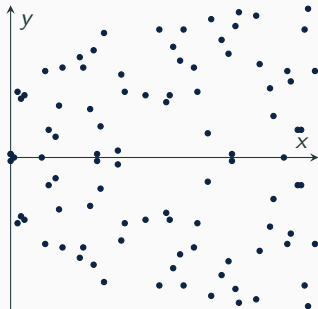
$$E : y^2 = x^3 - 2x + 1 \text{ over } \mathbb{R}$$



$$E : y^2 = x^3 - 2x + 1 \text{ over } \mathbb{R}$$



$$E : y^2 = x^3 - 2x + 1 \text{ over } \mathbb{F}_{89}$$



- Reducing the coefficients of E modulo p yields a cubic \tilde{E}

- Reducing the coefficients of E modulo p yields a cubic \tilde{E}
- If $\Delta_{\tilde{E}} \neq 0$ then we say that E has *good reduction* at p

- Reducing the coefficients of E modulo p yields a cubic \tilde{E}
- If $\Delta_{\tilde{E}} \neq 0$ then we say that E has *good reduction* at p
- If $\Delta_{\tilde{E}} = 0$ then we say that E has *bad reduction* at p

- Reducing the coefficients of E modulo p yields a cubic \tilde{E}
- If $\Delta_{\tilde{E}} \neq 0$ then we say that E has *good reduction* at p
- If $\Delta_{\tilde{E}} = 0$ then we say that E has *bad reduction* at p
- $\Delta_E = p_1^{a_1} \cdots p_n^{a_n} \implies N = p_1^{b_1} \cdots p_n^{b_n}$

Computing Elliptic Curves

- **Shafarevich (1963):** There are at most finitely many elliptic curves having good reduction outside $S = \{p_1, \dots, p_v\}$

- **Shafarevich (1963)**: There are at most finitely many elliptic curves having good reduction outside $S = \{p_1, \dots, p_v\}$
- **Taniyama, Weil (1950s, 1960's)**: A conjecture about elliptic curves of conductor N

- **Shafarevich (1963)**: There are at most finitely many elliptic curves having good reduction outside $S = \{p_1, \dots, p_v\}$
- **Taniyama, Weil (1950s, 1960's)**: A conjecture about elliptic curves of conductor N
 - $S = \{2\}$: Ogg (1966)
 - $S = \{2, 3\}$: Coghlán (1967)
 - $S = \{p\}$ for certain small primes p : Setzer (1975)
 - $S = \{11\}$: Agrawal, Coates, Hunt, and van der Poorten (1980)

- Subsequent methods rely on the Modularity Theorem

- Subsequent methods rely on the Modularity Theorem
- All elliptic curves of conductor N have been determined for

- Subsequent methods rely on the Modularity Theorem
- All elliptic curves of conductor N have been determined for
 - Antwerp IV (1972): $N \leq 200$
 - Tingley (1975): $N \leq 320$
 - Cremona (2019): $N \leq 500000$

- Reduce problem to solving a number of Thue-Mahler equations

$$F(x, y) = c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3 = ap_1^{z_1} \cdots p_v^{z_v}$$

- Reduce problem to solving a number of Thue-Mahler equations

$$F(x, y) = c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3 = ap_1^{z_1} \cdots p_v^{z_v}$$

- Goal: compute all curves having conductor $N \leq 10^6$

- Reduce problem to solving a number of Thue-Mahler equations

$$F(x, y) = c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3 = ap_1^{z_1} \cdots p_v^{z_v}$$

- Ideal Goal: $N \leq 10^8$

Theorem (Bennett, G., Reznitzky)

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

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

and relatively prime integers u and v with

$$F(u, v) = c_0 u^3 + c_1 u^2 v + c_2 u v^2 + c_3 v^3 = 2^{\alpha_1} 3^{\beta_1} \prod_{p|N_0} p^{\kappa_p}$$

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

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

Theorem (Bennett, G., Rechnitzer)

Here, $N_1 \mid N_0$,

$$(\alpha_0, \alpha_1) = \begin{cases} (2, 0) \text{ or } (2, 3) & \text{if } \alpha = 0 \\ (3, \geq 3) \text{ or } (2, \geq 4) & \text{if } \alpha = 1 \\ (2, 1), (4, 0) \text{ or } (4, 1) & \text{if } \alpha = 2 \\ (2, 1), (2, 2), (3, 2), (4, 0) \text{ or } (4, 1) & \text{if } \alpha = 3 \\ (2, \geq 0), (3, \geq 2), (4, 0) \text{ or } (4, 1) & \text{if } \alpha = 4 \\ (2, 0) \text{ or } (3, 1) & \text{if } \alpha = 5 \\ (2, \geq 0), (3, \geq 1), (4, 0) \text{ or } (4, 1) & \text{if } \alpha = 6 \\ (3, 0) \text{ or } (4, 0) & \text{if } \alpha = 7 \\ (3, 1) & \text{if } \alpha = 8, \end{cases}$$

Theorem (Bennett, G., Rechnitzer)

$$(\beta_0, \beta_1) = \begin{cases} (0, 0) & \text{if } \beta = 0 \\ (0, \geq 1) \text{ or } (1, \geq 0) & \text{if } \beta = 1 \\ (3, 0), (0, \geq 0), \text{ or } (1, \geq 0) & \text{if } \beta = 2 \\ (\beta, 0) \text{ or } (\beta, 1) & \text{if } \beta \geq 3, \end{cases}$$

$$\mathcal{D} = \prod_{p \mid \gcd(c_4(E), c_6(E))} p^{\min\{[\nu_p(c_4(E))/2], [\nu_p(c_6(E))/3]\}},$$

and $\kappa_p \in \mathbb{Z}_{>0}$ with $\kappa_p \in \{0, 1\}$ whenever $p^2 \mid N_1$.

Further,

if $\beta_0 \geq 3$, then $3 \mid c_1$ and $3 \mid c_2$

and

if $\nu_p(N) = 1$, for $p \geq 3$, then $p \mid D_F F(u, v)$



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

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

1. Compute every 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

2. Solve the corresponding Thue-Mahler equations

- Let $S = \{2, 3, 5, 7, 11, 13\}$

- Let $S = \{2, 3, 5, 7, 11, 13\}$
- There are 7893 corresponding forms which need to be solved

- Let $S = \{2, 3, 5, 7, 11, 13\}$
- There are 7893 corresponding forms which need to be solved
 - $F(x, y) = 19x^3 + 69x^2y + 76xy^2 + 126y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5} \cdot 13^{z_6}$
 - $F(x, y) = 22x^3 + 22x^2y + 55xy^2 + 100y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5} \cdot 13^{z_6}$
 - $F(x, y) = 46x^3 + 24x^2y + 85xy^2 + 7y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5} \cdot 13^{z_6}$
 - $F(x, y) = 13x^3 + 3x^2y + 18xy^2 + 14y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5} \cdot 13^{z_6}$
 - $F(x, y) = 17x^3 + 36x^2y + 39xy^2 + 26y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5} \cdot 13^{z_6}$
 - $F(x, y) = 2x^3 + 18x^2y + 21xy^2 + 65y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5} \cdot 13^{z_6}$
 - $F(x, y) = x^3 + 12x^2y + 18xy^2 + 149y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 7^{z_4} \cdot 11^{z_5} \cdot 13^{z_6}$
 - \vdots

Applying the Thue-Mahler solver

- A nice example

$$x^3 + 3xy^2 + 44xy^2 + 66y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$$

- A less nice example

$$3x^3 + 3xy^2 + 44xy^2 + 66y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$$

- A nice example

$$x^3 + 3xy^2 + 44xy^2 + 66y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$$

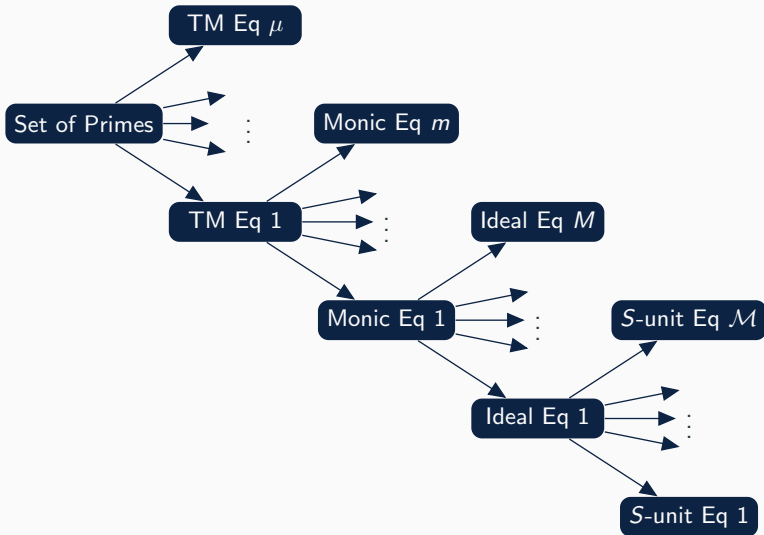
Total time: 247.580

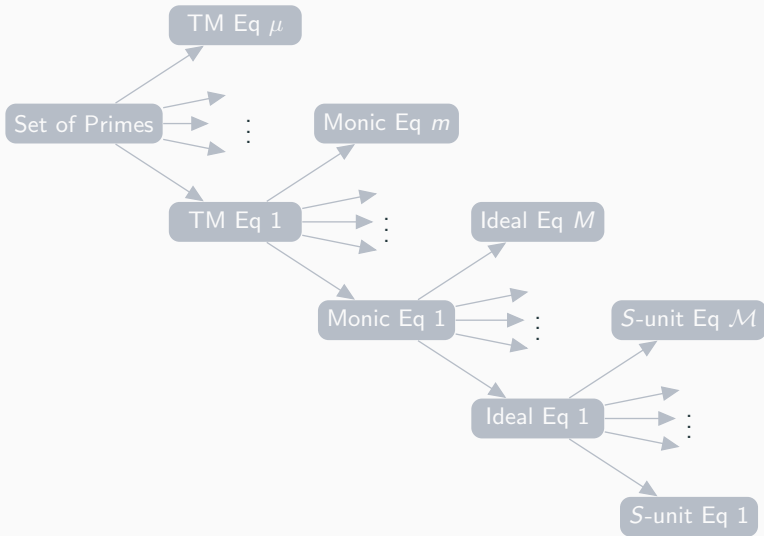
- A less nice example

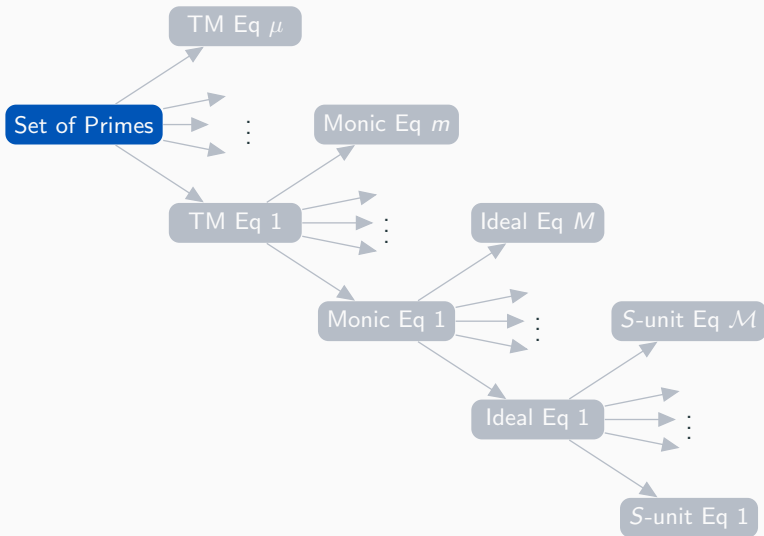
$$3x^3 + 3xy^2 + 44xy^2 + 66y^3 = 3^{z_1} \cdot 11^{z_2} \cdot 17^{z_3} \cdot 23^{z_4} \cdot 31^{z_5}$$

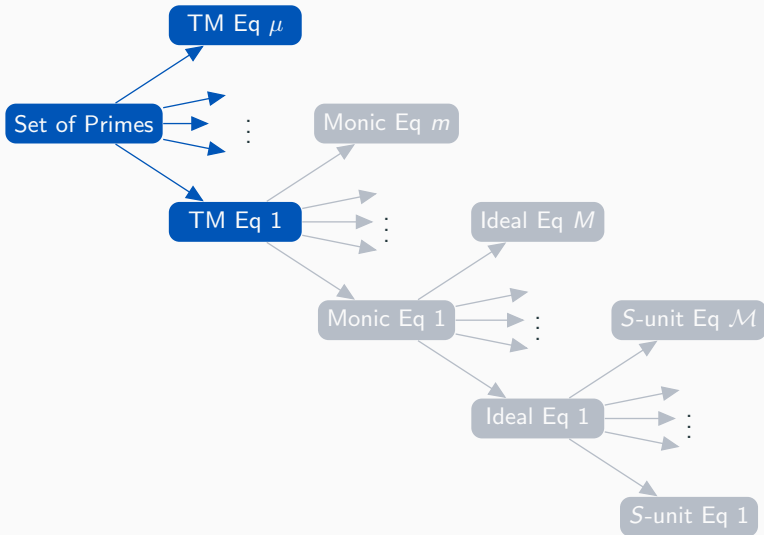
Total time: 2031.450

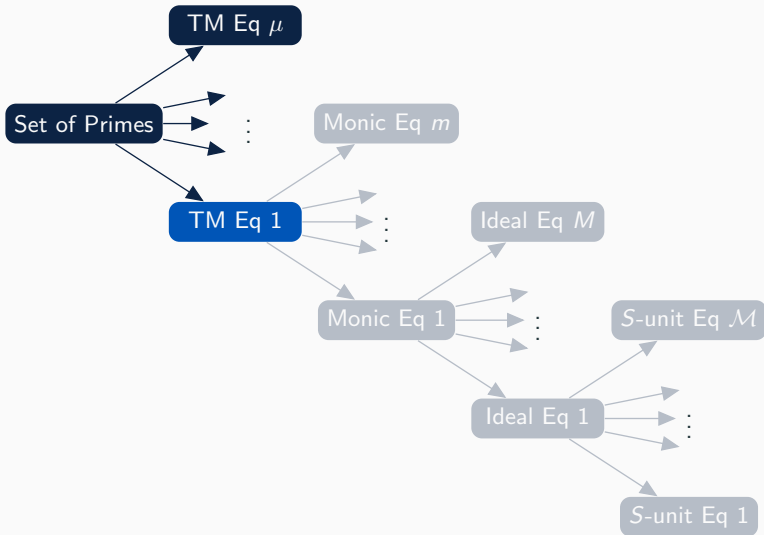
Algorithms for solving Thue-Mahler equations











- Fix $a \in \mathbb{Z}$ and a set of distinct rational primes $S = \{p_1, \dots, p_v\}$
- Reduce problem to solving a number of *Thue-Mahler equations*,

$$F(x, y) = c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3 = ap_1^{z_1} \cdots p_v^{z_v}$$

- Fix $a \in \mathbb{Z}$ and a set of distinct rational primes $S = \{p_1, \dots, p_v\}$
- Reduce problem to solving a number of *Thue-Mahler equations*,

$$F(x, y) = c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3 = ap_1^{z_1} \cdots p_v^{z_v}$$

- Without loss of generality, we may assume

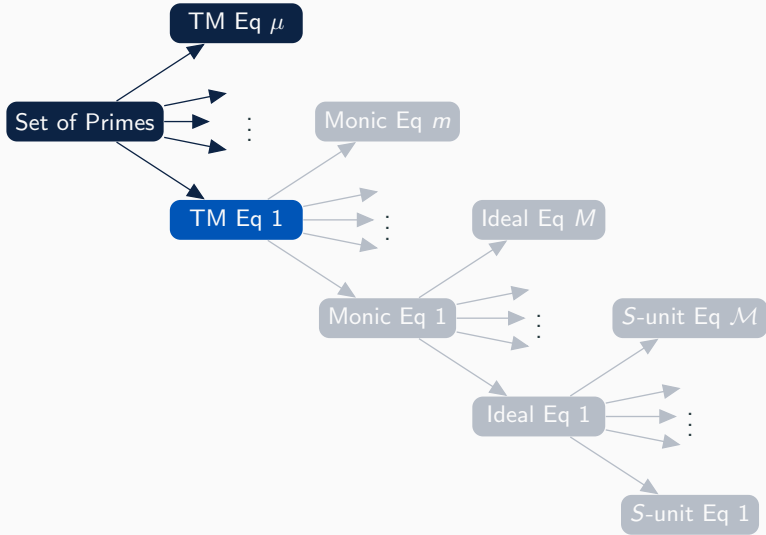
$$(x, y) = (y, c_0) = 1 \quad \text{and} \quad (a, p_1, \dots, p_v) = 1$$

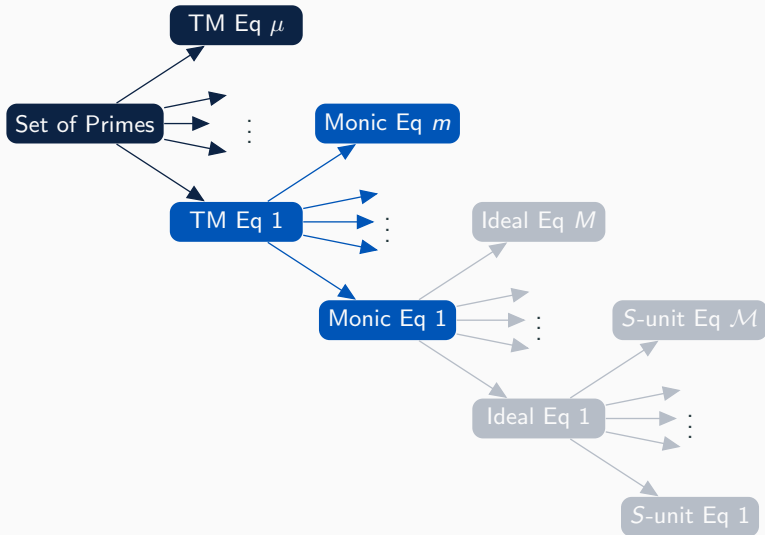
- Fix $a \in \mathbb{Z}$ and a set of distinct rational primes $S = \{p_1, \dots, p_v\}$
- Reduce problem to solving a number of *Thue-Mahler equations*,

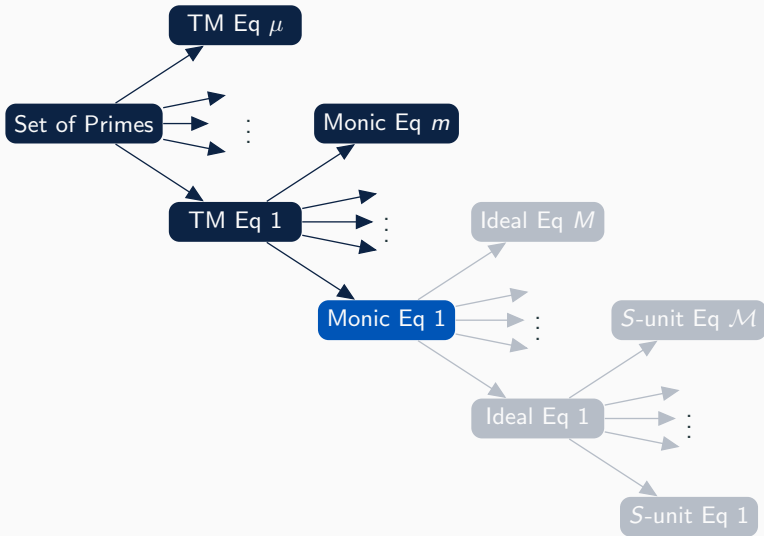
$$F(x, y) = x^3 + c_1x^2y + c_2xy^2 + c_3y^3 = ap_1^{z_1} \cdots p_v^{z_v}$$

- Without loss of generality, we may assume

$$(x, y) = 1 \quad \text{and} \quad (a, p_1, \dots, p_v) = 1$$







- Generate a number field K

- Generate a number field K
- Solving $F(x, y) = ap_1^{z_1} \cdots p_\nu^{z_\nu}$ is equivalent to solving a set of *ideal equations*

$$(x - y\theta)\mathcal{O}_K = \mathfrak{a}p_1^{u_1} \cdots p_\nu^{u_\nu}$$

where

- Generate a number field K
- Solving $F(x, y) = ap_1^{z_1} \cdots p_\nu^{z_\nu}$ is equivalent to solving a set of *ideal equations*

$$(x - y\theta)\mathcal{O}_K = \mathfrak{a}p_1^{u_1} \cdots p_\nu^{u_\nu}$$

where

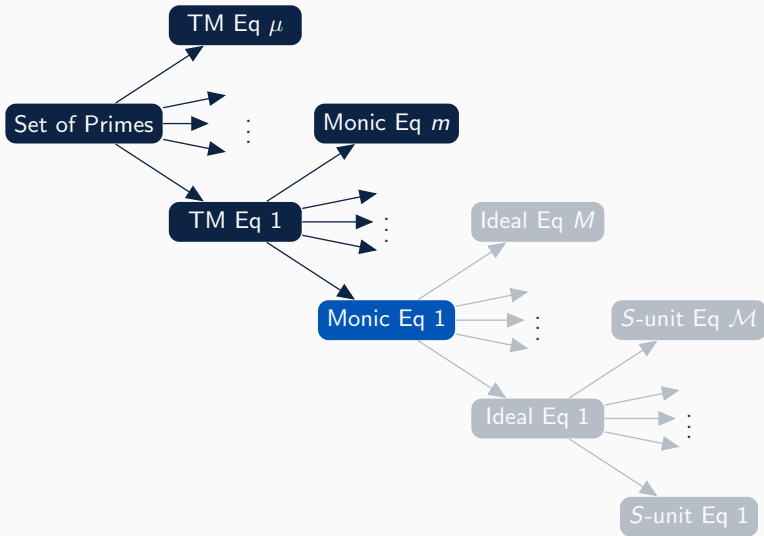
- \mathfrak{a}, p_i are determined by a, p_i

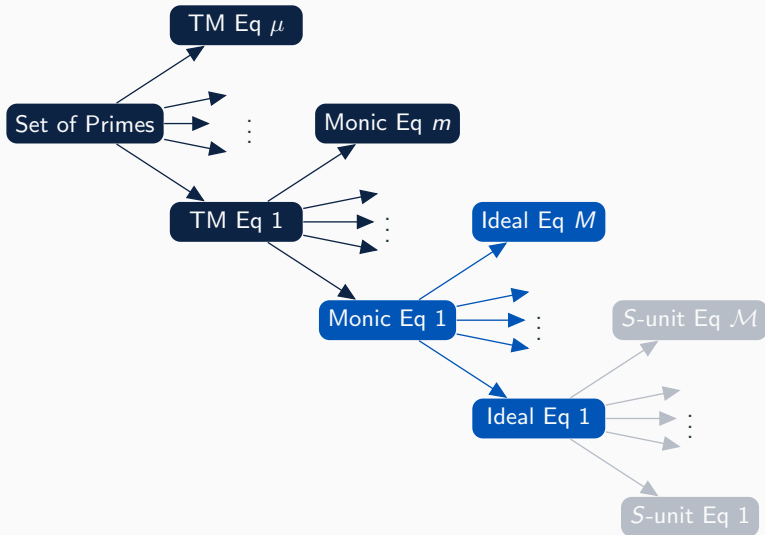
- Generate a number field K
- Solving $F(x, y) = ap_1^{z_1} \cdots p_\nu^{z_\nu}$ is equivalent to solving a set of *ideal equations*

$$(x - y\theta)\mathcal{O}_K = \mathfrak{a}p_1^{u_1} \cdots p_\nu^{u_\nu}$$

where

- \mathfrak{a}, p_i are determined by a, p_i
- x, y, u_i are unknown non-negative integers to be solved for





- A nice example

$$x^3 + 20xy^2 + 24xy^2 + 15y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}$$

- A less nice example

$$7x^3 + xy^2 + 29xy^2 - 25y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3}$$

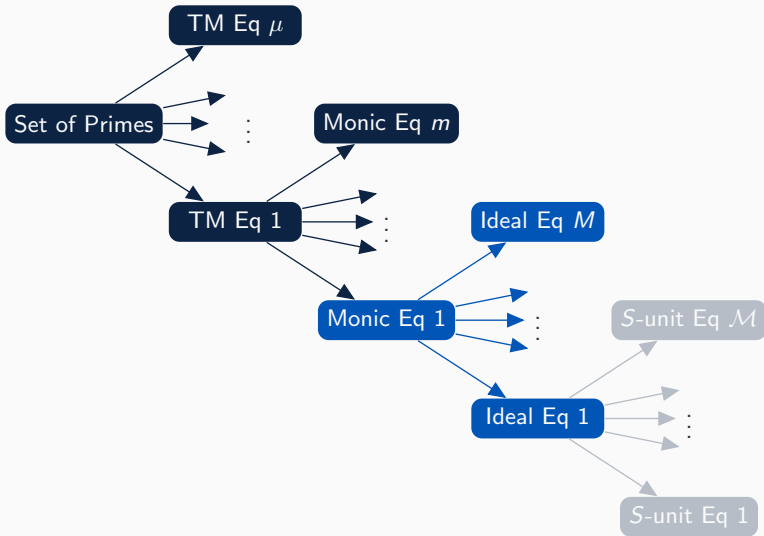
- A nice example

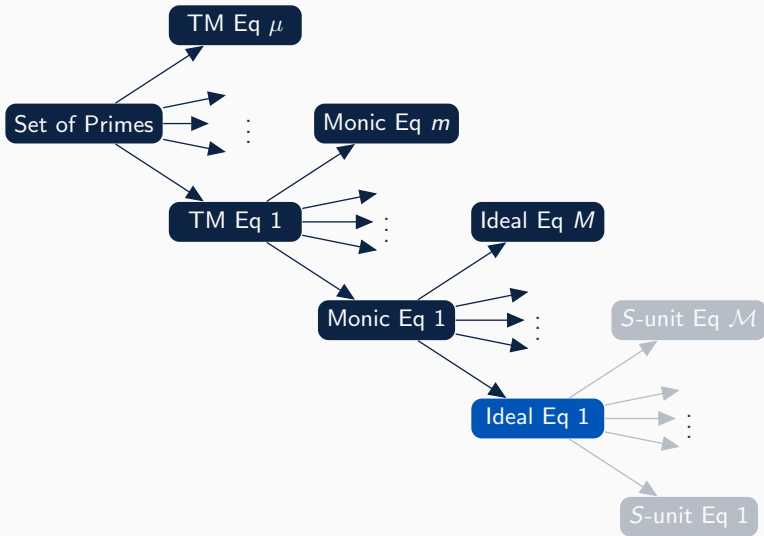
$$x^3 + 20xy^2 + 24xy^2 + 15y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}$$

- Number of Ideal Equations: 32
- A less nice example

$$7x^3 + xy^2 + 29xy^2 - 25y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3}$$

- Number of Ideal Equations: 26,136





- Applying a number of principalization tests, we are left with a set of *S-unit equations*

$$x - y\theta = \alpha \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu}$$

- Applying a number of principalization tests, we are left with a set of *S-unit equations*

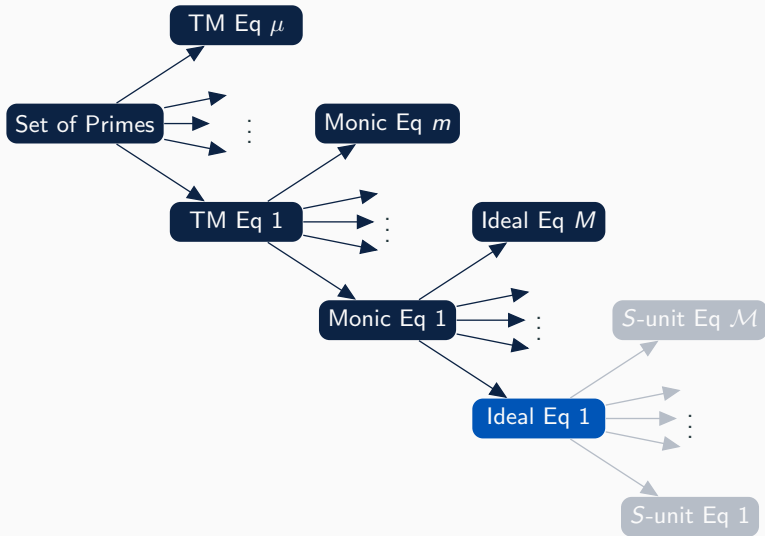
$$x - y\theta = \alpha \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu}$$

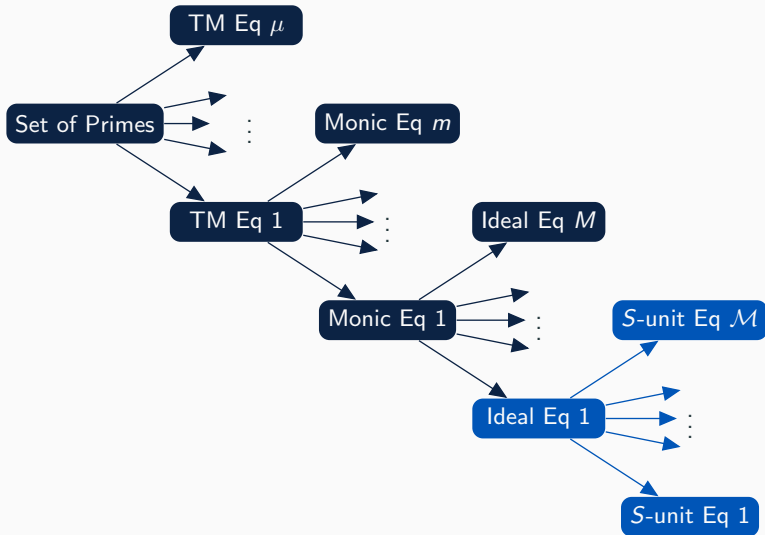
- $\alpha, \varepsilon_i, \gamma_i$ are computed directly from the ideal equation

- Applying a number of principalization tests, we are left with a set of *S-unit equations*

$$x - y\theta = \alpha \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu}$$

- $\alpha, \varepsilon_i, \gamma_i$ are computed directly from the ideal equation
- x, y, a_i, n_i are unknown





- A nice example

$$7x^3 + 12xy^2 + 14y^3 = 7^{z_1} \cdot 11^{z_2} \cdot 37^{z_3}$$

Number of ideal equations: 16

Number of principalization tests: 11,664

Number of S -unit equations: 1296

Total time: 21.5 seconds

- A less nice example

$$2x^3 + 20x^2y - 14xy^2 + 37y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 11^{z_4} \cdot 13^{z_5} \cdot 17^{z_6}$$

Number of ideal equations: 448

Number of principalization tests: 7,560,000

Number of S -unit equations: 139,264

Total time: 4 hours

- A really, really bad example

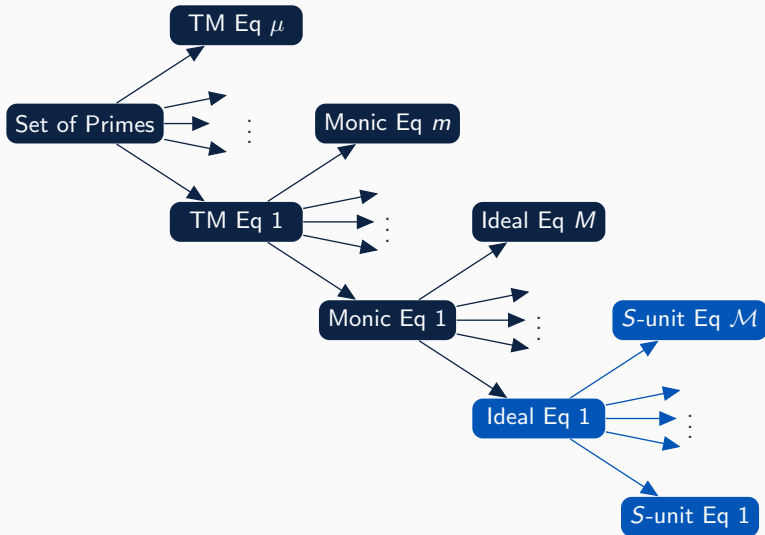
$$14x^3 + 20x^2y + 24xy^2 + 15y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}$$

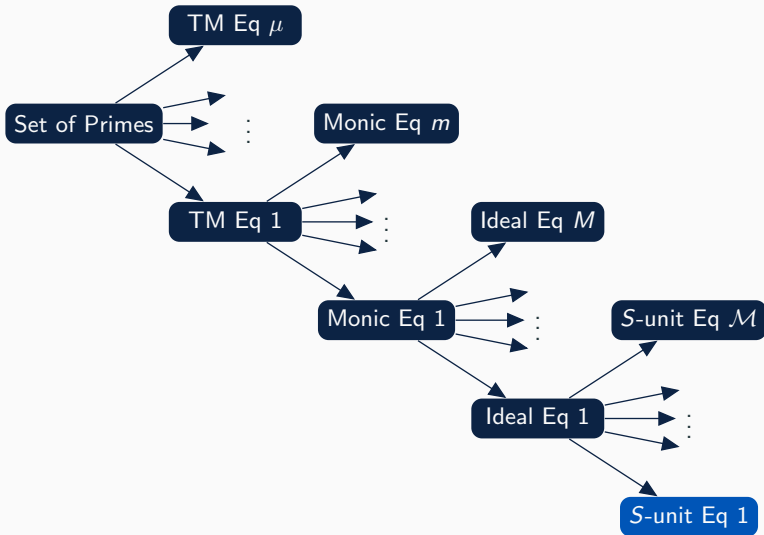
Number of ideal equations: 64

Number of principalization tests: 113,848,416

Number of S -unit equations: ????

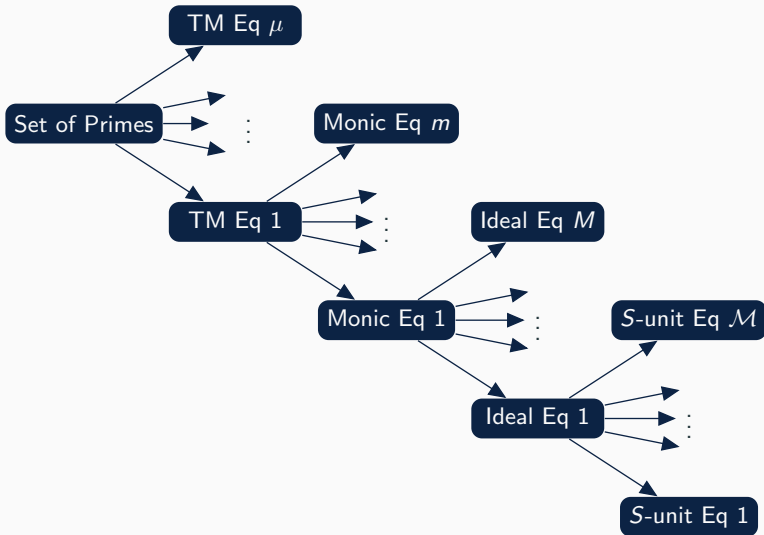
Total time: ????

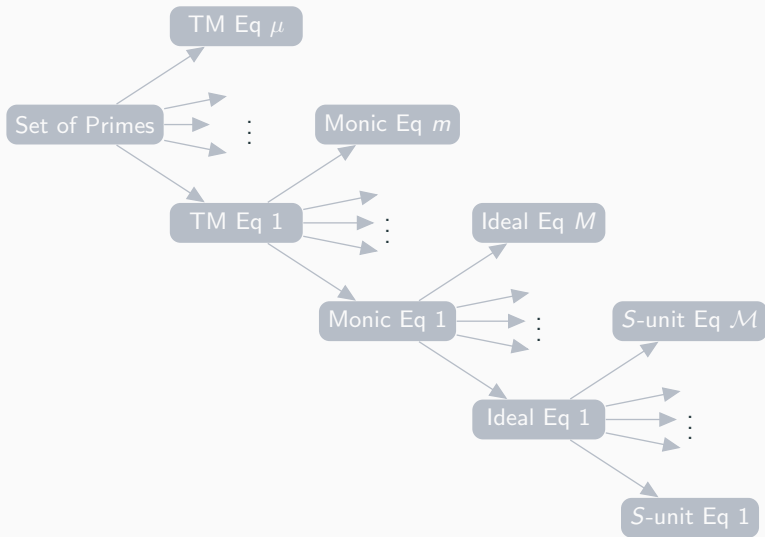


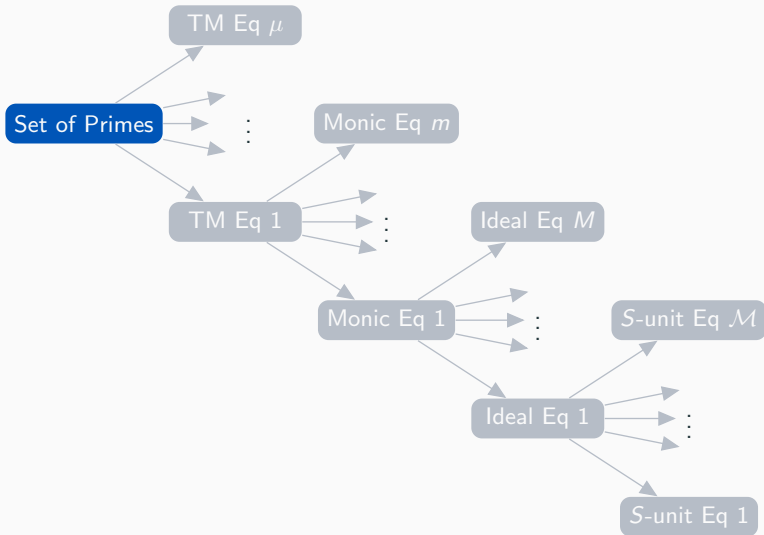


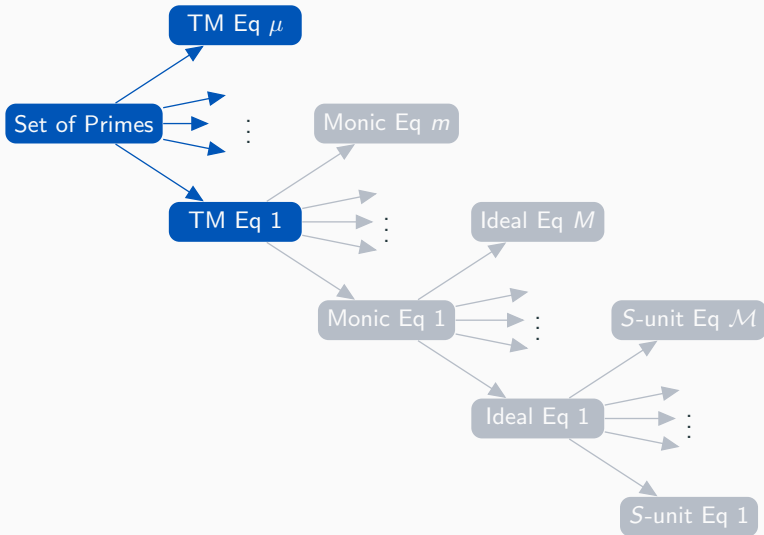
- Generate a very large upper bound on the solutions
- Reduce this bound
 - Compute all short vectors in a lattice
- Search below this reduced bound

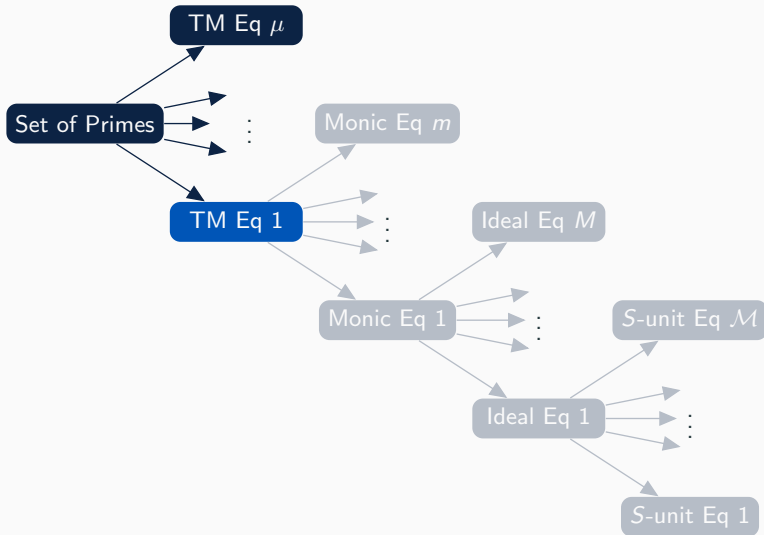
Refined algorithms for solving Thue-Mahler equations

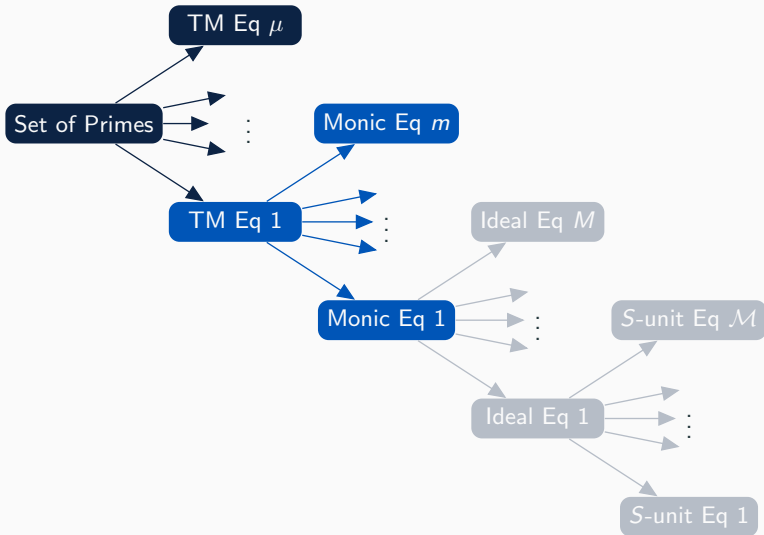


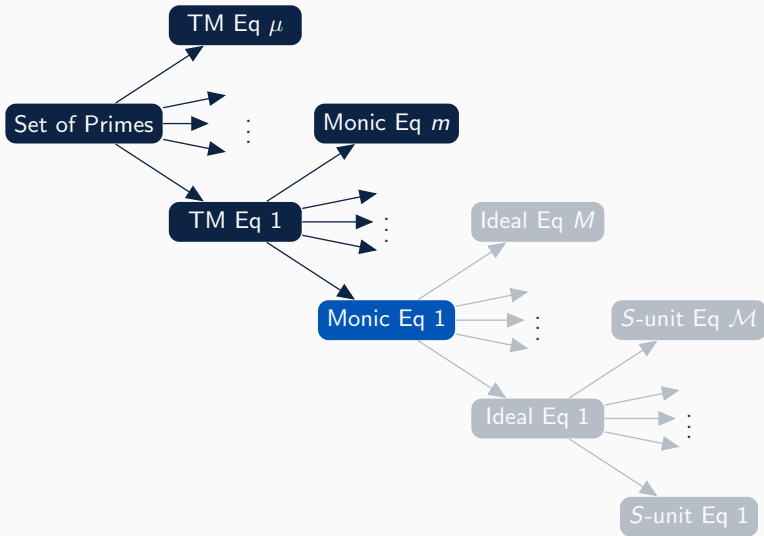












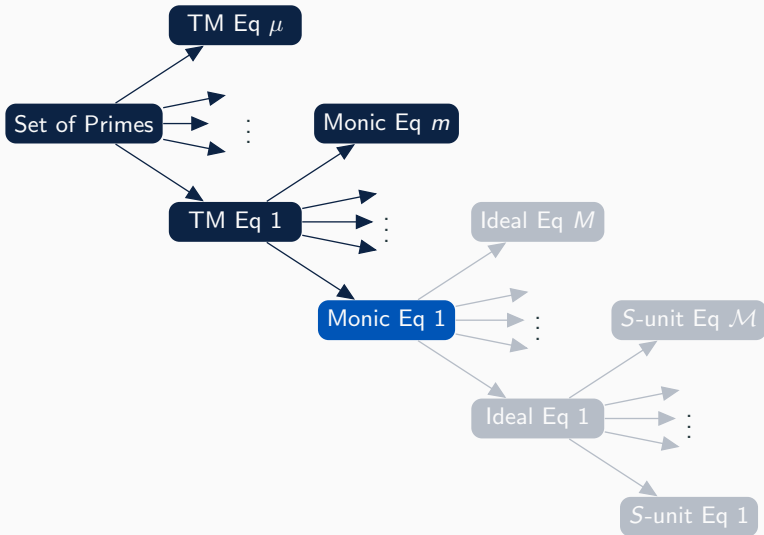
- Fewer ideal equations

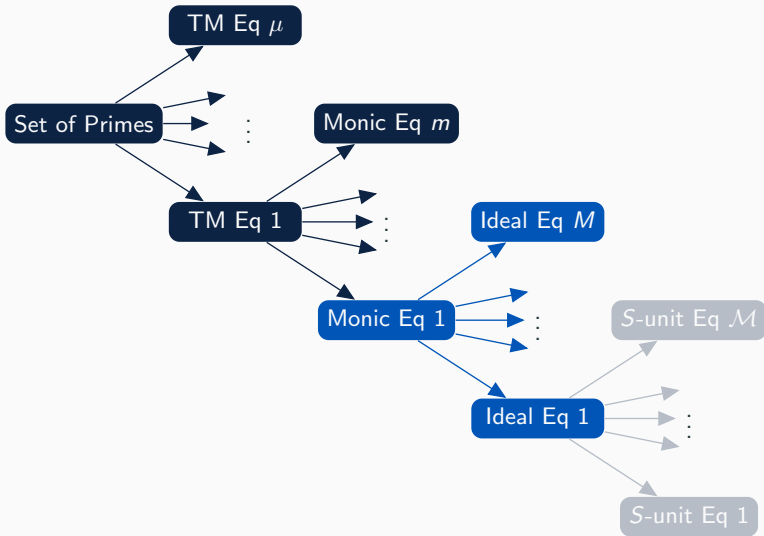
- Fewer ideal equations
- Fewer S -unit equations

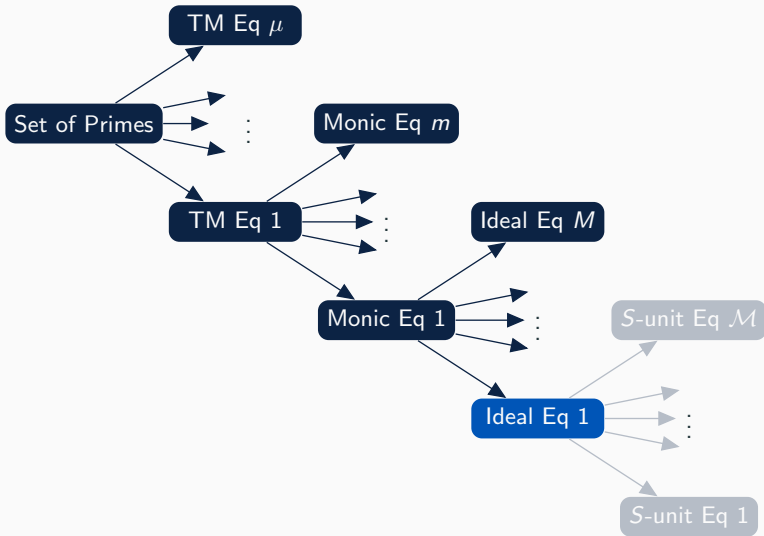
- Fewer ideal equations
- Fewer S -unit equations
 - Reduced test run-time

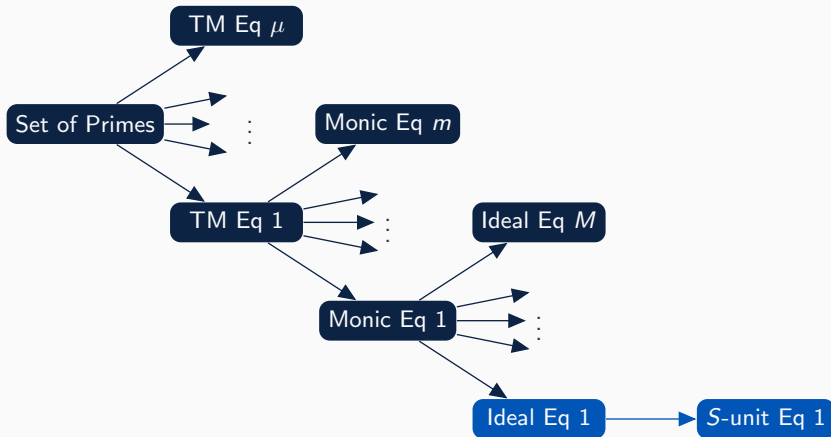
- Fewer ideal equations
- Fewer S -unit equations
 - Reduced test run-time
 - Yields only 1 S -unit equation for each ideal equation

- Fewer ideal equations
- Fewer S -unit equations
 - Reduced test run-time
 - Yields only 1 S -unit equation for each ideal equation
- Faster bound reduction for each S -unit equation









- A nice example

$$7x^3 + 12xy^2 + 14y^3 = 7^{z_1} \cdot 11^{z_2} \cdot 37^{z_3}$$

Number of ideal equations: 16

Number of principalization tests: 11,664

Number of S -unit equations: 1296

Total time: 21.5 seconds

- A nice example

$$7x^3 + 12xy^2 + 14y^3 = 7^{z_1} \cdot 11^{z_2} \cdot 37^{z_3}$$

Number of ideal equations: 16

Now: 8

Number of principalization tests: 11,664

Now: 8

Number of S -unit equations: 1296

Now: 8

Total time: 21.5 seconds

Now: 0.16 seconds

- A less nice example

$$2x^3 + 20x^2y - 14xy^2 + 37y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 11^{z_4} \cdot 13^{z_5} \cdot 17^{z_6}$$

Number of ideal equations: 448

Number of principalization tests: 7,560,000

Number of S -unit equations: 139,264

Total time: 4 hours

- A less nice example

$$2x^3 + 20x^2y - 14xy^2 + 37y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 5^{z_3} \cdot 11^{z_4} \cdot 13^{z_5} \cdot 17^{z_6}$$

Number of ideal equations: 448

Now: 64

Number of principalization tests: 7,560,000

Now: 64

Number of S -unit equations: 139,264

Now: 60

Total time: 4 hours

Now: 0.45 seconds

- This god-forsaken example

$$14x^3 + 20x^2y + 24xy^2 + 15y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}$$

Number of ideal equations: 64

Number of principalization tests: 113,848,416

Number of S -unit equations: ????

Total time: ????

- This god-forsaken example

$$14x^3 + 20x^2y + 24xy^2 + 15y^3 = 2^{z_1} \cdot 3^{z_2} \cdot 17^{z_3} \cdot 37^{z_4} \cdot 53^{z_5}$$

Number of ideal equations: 64

Now: 64

Number of principalization tests: 113,848,416

Now: 64

Number of S -unit equations: ????

Now: 60

Total time: ????

Now: 0.5 seconds

Current Ideas and Future Work

- Refine and optimize the Thue-Mahler solver at each S -unit equation

- Refine and optimize the Thue-Mahler solver at each S -unit equation
- Compute all elliptic curves of conductor $N < 10^6$

- Refine and optimize the Thue-Mahler solver at each S -unit equation
- Compute all elliptic curves of conductor $N < 10^6$
- Generalize the Thue-Mahler solver over number fields

Thank You