Solving S-unit equations in Sage and Applications to Algebraic Curves

Beth Malmskog
with Alejandra Alvarado, Angelos Koutsianas, Christopher Rasmussen, Christelle Vincent, and Mckenzie West

July 4, 2017

Diophantine Approximation and Algebraic Curves Conference at BIRS

A Motivating Problem

Definition

A smooth curve $\mathcal{P}$ defined by $y^3 = f(x)$ where $\deg(f)=4$ is called a Picard curve.

A Motivating Problem

Definition

A smooth curve $\mathcal{P}$ defined by $y^3 = f(x)$ where $\deg(f)=4$ is called a Picard curve.

Picard curves have genus 3.

Simplest non-hyperelliptic curves.

A Motivating Problem

Definition

A smooth curve $\mathcal{P}$ defined by $y^3 = f(x)$ where $\deg(f)=4$ is called a Picard curve.

Picard curves have genus 3.

Simplest non-hyperelliptic curves.

Definition

A smooth, irreducible curve $\mathcal{C}$ defined over $\mathbb{Q}$ is said to have good reduction at a prime p if there exists a model of $\mathcal{C}$ such that the defining equations reduced modulo p define a smooth, irreducible curve $\mathcal{C}_p$.

A Motivating Problem

Definition

A smooth curve $\mathcal{P}$ defined by $y^3 = f(x)$ where $\deg(f)=4$ is called a Picard curve.

Picard curves have genus 3.

Simplest non-hyperelliptic curves.

Definition

A smooth, irreducible curve $\mathcal{C}$ defined over $\mathbb{Q}$ is said to have good reduction at a prime p if there exists a model of $\mathcal{C}$ such that the defining equations reduced modulo p define a smooth, irreducible curve $\mathcal{C}_p$.

Malmskog-Rasmussen goal: Find all Picard curves defined over $\mathbb{Q}$ with good reduction at all primes except $p = 3$.

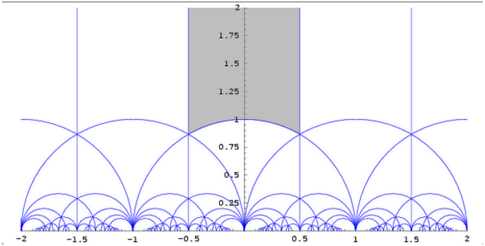
Bőrner-Bouw-Wewers: All Picard curves over $\mathbb{Q}$ have bad reduction at $p = 3$.

Reduction Properties–Why Care?

- Ihara's question

Reduction Properties–Why Care?

- Ihara's question



- Every quotient curve of the modular curve $\mathcal{X}_0(N)$ has good reduction except at primes dividing N.

Our Roadmap

1996 Smart–Found all genus 2 curves over $\mathbb{Q}$ with good reduction at all primes except $p = 2$.

We generalize methods, equivalence of binary forms to Picard curves.

Our Roadmap

1996 Smart–Found all genus 2 curves over $\mathbb{Q}$ with good reduction at all primes except $p = 2$.

We generalize methods, equivalence of binary forms to Picard curves.

Key step: Enumeration of all solutions to the equation

$$x + y = 1$$

where $x, y \in \mathcal{O}_S^\times$, and S is a set of primes in $K/\mathbb{Q}$.

Our Roadmap

1996 Smart–Found all genus 2 curves over $\mathbb{Q}$ with good reduction at all primes except $p = 2$.

We generalize methods, equivalence of binary forms to Picard curves.

Key step: Enumeration of all solutions to the equation

$$x + y = 1$$

where $x, y \in \mathcal{O}_S^\times$, and S is a set of primes in $K/\mathbb{Q}$.
New Goal: Create self-contained functions to solve S-unit equation.

S-units

$$\begin{array}{ccccc} K & \mathbb{Z}_K & S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{t_1}, \infty_1, \ldots, \infty_{t_2}\} & \mathcal{O}_S = \mathbb{Z}_K[1/\mathfrak{p}_1, \ldots, 1/\mathfrak{p}_{t_1}] & \mathcal{O}_S^* \\ | & | & | & | & | \\ \mathbb{Q} & \mathbb{Z} & S_{\mathbb{Q}} = \{p_1, \ldots, p_s, \infty\} & \mathcal{O}_{S_{\mathbb{Q}}} = \mathbb{Z}[1/p_1, \ldots, 1/p_s] & \mathcal{O}_{S_{\mathbb{Q}}}^{\times} \end{array}$$

S-units

$$\begin{array}{ccccc} K & \mathbb{Z}_K & S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{t_1}, \infty_1, \ldots, \infty_{t_2}\} & \mathcal{O}_S = \mathbb{Z}_K[1/\mathfrak{p}_1, \ldots, 1/\mathfrak{p}_{t_1}] & \mathcal{O}_S^* \\ | & | & | & | & | \\ \mathbb{Q} & \mathbb{Z} & S_{\mathbb{Q}} = \{p_1, \ldots, p_s, \infty\} & \mathcal{O}_{S_{\mathbb{Q}}} = \mathbb{Z}[1/p_1, \ldots, 1/p_s] & \mathcal{O}_{S_{\mathbb{Q}}}^\times \end{array}$$

$S_{\mathbb{Q}} = \{3, \infty\}$,

$$\mathcal{O}_{S_{\mathbb{Q}}}^\times = \left\{\ldots, \pm\frac{1}{9}, \pm\frac{1}{3}, \pm 1, \pm 3, \pm 9, \ldots\right\}$$

$$= \left\{(-1)^{a_1} 3^{a_2} : (a_1, a_2) \in \mathbb{Z}^2\right\}.$$

S-units

$$\begin{array}{cccccc} K & \mathbb{Z}_K & S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{t_1}, \infty_1, \ldots, \infty_{t_2}\} & \mathcal{O}_S = \mathbb{Z}_K[1/\mathfrak{p}_1, \ldots, 1/\mathfrak{p}_{t_1}] & \mathcal{O}_S^* \\ | & | & | & | & | \\ \mathbb{Q} & \mathbb{Z} & S_{\mathbb{Q}} = \{p_1, \ldots, p_s, \infty\} & \mathcal{O}_{S_{\mathbb{Q}}} = \mathbb{Z}[1/p_1, \ldots, 1/p_s] & \mathcal{O}_{S_{\mathbb{Q}}}^\times \end{array}$$

$S_{\mathbb{Q}} = \{3, \infty\}$,

$$\begin{aligned} \mathcal{O}_{S_{\mathbb{Q}}}^\times &= \left\{ \ldots, \pm\frac{1}{9}, \pm\frac{1}{3}, \pm 1, \pm 3, \pm 9, \ldots \right\} \\ &= \left\{ (-1)^{a_1} 3^{a_2} : (a_1, a_2) \in \mathbb{Z}^2 \right\}. \end{aligned}$$

Let $K = \mathbb{Q}(\xi)$, where $\xi^6 + 3 = 0$, so $(3) = (\xi)^6$.

$S = \{(\xi), \infty_1, \ldots, \infty_4\}$.

$$\mathcal{O}_S^\times = \left\{ \zeta_6^{a_1} \xi^{a_2} (\frac{1}{2}\xi^5 - \frac{1}{2}\xi^2 - \xi - 1)^{a_3} (\frac{1}{2}\xi^4 - \frac{1}{2}\xi^3 + \xi^2 - \frac{1}{2}\xi + \frac{1}{2})^{a_4} : (a_1, a_2, a_3, a_4) \in \mathbb{Z}^4 \right\}.$$

Solving the S-Unit Equation

- 1939 Dirichlet–S-unit group is finitely generated (rank $r + s$).
- 1909-1921-1955 Thue, Siegel, Roth–There are finitely many rational numbers of bounded height within a given distance of an irrational algebraic number.
- 1966 Baker–Lower bound on linear combination of logarithms of algebraic α_i based on heights of coefficients and α_is.
- 1972-1979 Győry–Explicit bound, using Baker's method.
- 1987-1992 de Weger, Tzanakis-de Weger–Use LLL to greatly reduce bounds
- 1989 Yu–Linear forms in p-adic logarithms
- 1996-1999 Wildanger, Smart–Efficient enumeration of solutions

Big Picture

Let $\mathcal{O}_S = \langle \rho_0, \ldots, \rho_t \rangle$, where ρ_0 is a root of unity. To solve

$$x + y = 1,$$

where $x = \prod \rho_i^{a_{i,x}}$, $y = \prod \rho_i^{a_{i,y}}$, need to bound exponents and search over finite space. Three main steps:

1. Find a ridiculously large bound
2. Use LLL to greatly reduce bound
3. Somehow find all solutions in smaller search space. For us, this means sieving.

Big Picture

Let $\mathcal{O}_S = \langle \rho_0, \ldots, \rho_t \rangle$, where ρ_0 is a root of unity. To solve

$$x + y = 1,$$

where $x = \prod \rho_i^{a_{i,x}}$, $y = \prod \rho_i^{a_{i,y}}$, need to bound exponents and search over finite space. Three main steps:

1. Find a ridiculously large bound
2. Use LLL to greatly reduce bound
3. Somehow find all solutions in smaller search space. For us, this means sieving.

Caveat: Need to consider prime associated to minimum absolute value of term with maximum exponent...

Step 1: A Closer Look at Baker's Theorem

Theorem (Baker-Wüstholz, 1993)

Let L be a linear form in $t+1$ variables, and let $\rho_0, \ldots, \rho_t \in \overline{\mathbb{Q}} - \{0,1\}$ with linearly independent logs. Let B be the subfield of $\overline{\mathbb{Q}}$ generated by the ρ_i. If

$$\Lambda = L(\log \rho_0, \log \rho_1, \ldots, \log \rho_t) \neq 0,$$

then

$$\log |\Lambda| > -C(t, n_B) h'(L) \prod_{j=0}^{t} h'(\rho_j),$$

where the constant $C(t, n_B)$ is defined by

$$C(t, n_B) = 18(t+2)!(t+1)^{(t+2)}(32 n_B)^{(t+3)} \log\left(2(t+1)n_B\right).$$

A Simpler Look at Baker and S-Unit Solutions

Assume that

Baker-Wüstholz: If L is a linear form, $\Lambda = L(\log \rho_0, \log \rho_1, \ldots, \log \rho_t) \neq 0$, then

$$\log |\Lambda| > -C_1 h'(L) \prod_{j=0}^{t} h'(\rho_j).$$

A Simpler Look at Baker and S-Unit Solutions

Assume that

Baker-Wüstholz: If L is a linear form, $\Lambda = L(\log \rho_0, \log \rho_1, \ldots, \log \rho_t) \neq 0$, then

$$\log |\Lambda| > -C_1 h'(L) \prod_{j=0}^{t} h'(\rho_j).$$

Rewrite our S-unit equation:

$$x + y = 1 \Rightarrow \frac{x}{y} = \frac{1}{y} - 1 \neq 1,$$

A Simpler Look at Baker and S-Unit Solutions

Assume that

Baker-Wüstholz: If L is a linear form, $\Lambda = L(\log \rho_0, \log \rho_1, \ldots, \log \rho_t) \neq 0$, then

$$\log |\Lambda| > -C_1 h'(L) \prod_{j=0}^{t} h'(\rho_j).$$

Rewrite our S-unit equation:

$$x + y = 1 \Rightarrow \frac{x}{y} = \frac{1}{y} - 1 \neq 1, \text{ so}$$

$$\begin{aligned} \prod_{i=0}^{t} \rho_i^{a_i} &= \frac{1}{y} - y \neq 1. \\ \sum_{i=0}^{t} a_i \log(\rho_i) &= \Lambda \neq 0, \end{aligned}$$

where α_i are S-units generators, a_i are exponents. We want to bound a_i.

A Large Bound

Fix $\psi \colon K \hookrightarrow \mathbb{C}$. Let $H = \max\{|a_i| : 0 \leq i \leq t\}$

Ignoring all details:

$$h'(L) > C_2 \log(H) \text{ and } C_3 = \prod_{i=0}^{t} h'(\alpha_i).$$

Baker-Wustholz:

$$\log|\Lambda| > -C_1 C_2 \log(H) C_3$$
$$|\Lambda| > e^{-C_4 \log(H)}$$

A Large Bound

Fix $\psi \colon K \hookrightarrow \mathbb{C}$. Let $H = \max\{|a_i| : 0 \le i \le t\}$

Ignoring all details:

$$h'(L) > C_2 \log(H) \text{ and } C_3 = \prod_{i=0}^{t} h'(\alpha_i).$$

Baker-Wustholz:

$$\log|\Lambda| > -C_1 C_2 \log(H) C_3$$
$$|\Lambda| > e^{-C_4 \log(H)}$$

Geometric argument: $|\Lambda| < C_5 e^{-C_6 H}$

$$e^{-C_4 \log(H)} < |\Lambda| < C_5 e^{-C_6 H},$$

$$C_4 \log(H) > -\log(C_5) + C_6 H.$$

A Large Bound

Fix $\psi \colon K \hookrightarrow \mathbb{C}$. Let $H = \max\{|a_i| : 0 \le i \le t\}$

Ignoring all details:

$$h'(L) > C_2 \log(H) \text{ and } C_3 = \prod_{i=0}^{t} h'(\alpha_i).$$

Baker-Wustholz:

$$\log|\Lambda| > -C_1 C_2 \log(H) C_3$$
$$|\Lambda| > e^{-C_4 \log(H)}$$

Geometric argument: $|\Lambda| < C_5 e^{-C_6 H}$

$$e^{-C_4 \log(H)} < |\Lambda| < C_5 e^{-C_6 H},$$

$$C_4 \log(H) > -\log(C_5) + C_6 H.$$

Pethö-de Weger $\Rightarrow H < K_0$.

A Large Bound

Fix $\psi\colon K \hookrightarrow \mathbb{C}$. Let $H = \max\{|a_i| : 0 \le i \le t\}$

Ignoring all details:

$$h'(L) > C_2 \log(H) \text{ and } C_3 = \prod_{i=0}^{t} h'(\alpha_i).$$

Baker-Wustholz:

$$\log|\Lambda| > -C_1 C_2 \log(H) C_3$$
$$|\Lambda| > e^{-C_4 \log(H)}$$

Geometric argument: $|\Lambda| < C_5 e^{-C_6 H}$

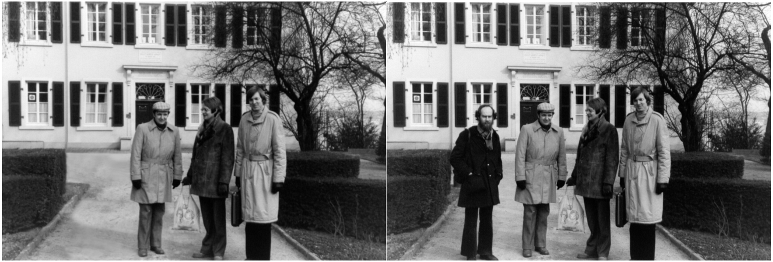
$$e^{-C_4 \log(H)} < |\Lambda| < C_5 e^{-C_6 H},$$

$$C_4 \log(H) > -\log(C_5) + C_6 H.$$

Pethö-de Weger $\Rightarrow H < K_0$.

Problem: For one of our fields, $K_0 = 2.137374 \times 10^{19}$.

Step 2: LLL



LLL: lattice basis reduction algorithm devised in 1982 by Henrik Lenstra, Arjen Lenstra, and Laslo Lovász.

Applying LLL reduction to a particular lattice yields a bound $K_1 \approx \log(K_0)$. Can be repeated with new bound until there is no further improvement.

LLL in Action: Picard Curves

Need all $K/\mathbb{Q}$ with degree ≤ 4 and $\text{Disc}(K) \in \mathcal{O}_S^\times$ with $S = \{3, \infty\}$.

Field	Degree	Minimal Polynomial	K_0	K_1
M_0	1	$x - 1$	4.916825×10^9	3
M_1	2	$x^2 + x + 1$	8.018712×10^9	5
M_2	3	$x^3 - 3x + 1$	2.067269×10^{19}	217
M_3	3	$x^3 - 3$	1.957261×10^{15}	49
M_3'	3			
M_3''	3			
L_3	6	$x^6 + 3$	2.137374×10^{19}	243

All fields have class number 1.

(3) is totally ramified in all (non-trivial) extensions.

Step 3: Sieving for Solutions

A sieve:

Recall $\mathcal{O}_S^\times = \langle \rho_0, \ldots, \rho_t \rangle$, where ρ_0 is a root of unity. Say that

$$x + y = 1,$$

where

$$x = \prod \rho_i^{a_{i,x}} = \rho^{\mathbf{a_x}}, \qquad y = \prod \rho_i^{a_{i,y}} = \rho^{\mathbf{a_y}}.$$

Step 3: Sieving for Solutions

A sieve:

Recall $\mathcal{O}_S^\times = \langle \rho_0, \ldots, \rho_t \rangle$, where ρ_0 is a root of unity. Say that

$$x + y = 1,$$

where

$$x = \prod \rho_i^{a_{i,x}} = \rho^{\mathbf{a_x}}, \qquad y = \prod \rho_i^{a_{i,y}} = \rho^{\mathbf{a_y}}.$$

Let q be a prime of $\mathbb{Q}$ which splits completely in K, so

$$q\mathcal{O}_K = \mathfrak{q}_0 \ldots \mathfrak{q}_{n-1}.$$

We now consider the image of the equation $x + y = 1$ modulo $\mathfrak{q}_j$ for each j, $0 \leq j \leq n-1$, where $\overline{\alpha}$ denotes the reduction modulo $\mathfrak{q}_j$. Let

$$\overline{\rho} = (\overline{\rho_0}, \ldots, \overline{\rho_t}) \in \left(\mathbb{F}_q^\times\right)^{t+1}.$$

Step 3: Sieving for Solutions

A sieve:

Recall $\mathcal{O}_S^\times = \langle \rho_0, \ldots, \rho_t \rangle$, where ρ_0 is a root of unity. Say that

$$x + y = 1,$$

where

$$x = \prod \rho_i^{a_{i,x}} = \rho^{\mathbf{a_x}}, \qquad y = \prod \rho_i^{a_{i,y}} = \rho^{\mathbf{a_y}}.$$

Let q be a prime of $\mathbb{Q}$ which splits completely in K, so

$$q\mathcal{O}_K = \mathfrak{q}_0 \ldots \mathfrak{q}_{n-1}.$$

We now consider the image of the equation $x + y = 1$ modulo $\mathfrak{q}_j$ for each j, $0 \leq j \leq n-1$, where $\overline{\alpha}$ denotes the reduction modulo $\mathfrak{q}_j$. Let

$$\overline{\rho} = (\overline{\rho_0}, \ldots, \overline{\rho_t}) \in \left(\mathbb{F}_q^\times\right)^{t+1}.$$

Then we have

$$\overline{\rho}^{\mathbf{a_x}} + \overline{\rho}^{\mathbf{a_y}} = \mathbf{1}$$

for all j, which gives a set of conditions on $\mathbf{a_x}$ and $\mathbf{a_y}$ modulo $q-1$.

Sieve continued

Choosing a list of split primes $q_1, q_2, \ldots q_N$ so that

$$\mathrm{lcm}(q_1, q_2, \ldots q_N) > 2K_1,$$

can use Chinese remainder-type argument to find searchable space of potential exponent vectors in $\mathbb{Z}^{t+1}$.

Sieve continued

Choosing a list of split primes $q_1, q_2, \ldots q_N$ so that

$$\mathrm{lcm}(q_1, q_2, \ldots q_N) > 2K_1,$$

can use Chinese remainder-type argument to find searchable space of potential exponent vectors in $\mathbb{Z}^{t+1}$.

Finally, check whether each exponent vector yields an actual S-unit solution.

Note: This is not the same method introduced by Wildanger and improved by Smart.

Results and Beyond

Picard curves: Implementing the above routines in Sage, we solved the S-unit equation in the above-listed fields, yielding 63 $\mathbb{Q}$-isomorphism classes of Picard curves with good reduction away from $p = 3$.

Results and Beyond

Picard curves: Implementing the above routines in Sage, we solved the S-unit equation in the above-listed fields, yielding 63 $\mathbb{Q}$-isomorphism classes of Picard curves with good reduction away from $p = 3$.

Note: Proved a result that eliminated p-adic case for our problem, so implementation included a special case of LLL but general sieve.

Results and Beyond

Picard curves: Implementing the above routines in Sage, we solved the S-unit equation in the above-listed fields, yielding 63 $\mathbb{Q}$-isomorphism classes of Picard curves with good reduction away from $p = 3$.

Note: Proved a result that eliminated p-adic case for our problem, so implementation included a special case of LLL but general sieve.

2015/2016: Angelos Koutsianas: all elliptic curves with good reduction outside S defined over a general number field.

Note: Koutsianas also implemented S-unit solving in Sage, including both cases of LLL but avoiding sieve.

General Sage Implementation

Collaborate@ICERM January 2017

Team: Alejandra Alvarado, Angelos Koutsianas, M., Chris Rasmussen, Christelle Vincent, Mckenzie West (with moral support from Bjorn Poonen)

Implemented function to solve $x + y = 1$ for general number field K and set S.

SageTrac Ticket #22148

Computational Comparison

Smart, 1997 (paraphrased)

- The algorithm was implemented on a network of 20 SUN workstations, written in C++. Issues with load balancing and computer failure had to be navigated.
- The program took around 27 MIPS-years, or in real life, about 18 days.

Computational Comparison

Smart, 1997 (paraphrased)

- The algorithm was implemented on a network of 20 SUN workstations, written in C++. Issues with load balancing and computer failure had to be navigated.
- The program took around 27 MIPS-years, or in real life, about 18 days.

M.-Rasmussen, 2015

- Under 2000 lines of Sage code.
- Ran in approximately 1 day on 1 desktop machine.

Computational Comparison

Smart, 1997 (paraphrased)

- The algorithm was implemented on a network of 20 SUN workstations, written in C++. Issues with load balancing and computer failure had to be navigated.
- The program took around 27 MIPS-years, or in real life, about 18 days.

M.-Rasmussen, 2015

- Under 2000 lines of Sage code.
- Ran in approximately 1 day on 1 desktop machine.

Alvarado-Koutsianas-M.-Rasmussen-Vincent-West, 2017

- General solver is approximately 3000 lines of Sage code.
- Some problems run in seconds, others in minutes, others...

Next

- Improving Sage implementation:
  - Incorporate bound improvements from literature
  - More general linear equations
  - Improve bound reduction using de Weger
  - Implement Wildanger/Smart
  - Make code better!

Next

- Improving Sage implementation:
  - Incorporate bound improvements from literature
  - More general linear equations
  - Improve bound reduction using de Weger
  - Implement Wildanger/Smart
  - Make code better!
- What can we do with this function?
  - Genus 2 curves good away from 3: Andrew Sutherland, Borys Kadets, James Rowan with $2, 3 \in S$

Next

- Improving Sage implementation:
  - Incorporate bound improvements from literature
  - More general linear equations
  - Improve bound reduction using de Weger
  - Implement Wildanger/Smart
  - Make code better!
- What can we do with this function?
  - Genus 2 curves good away from 3: Andrew Sutherland, Borys Kadets, James Rowan with $2, 3 \in S$
  - $p = 5$ Chris Rasmussen and Ryan Karpisz
  - $p = 7, 11 \ldots$

Next

- Improving Sage implementation:
  - Incorporate bound improvements from literature
  - More general linear equations
  - Improve bound reduction using de Weger
  - Implement Wildanger/Smart
  - Make code better!
- What can we do with this function?
  - Genus 2 curves good away from 3: Andrew Sutherland, Borys Kadets, James Rowan with $2, 3 \in S$
  - $p = 5$ Chris Rasmussen and Ryan Karpisz
  - $p = 7, 11 \ldots$
  - ...

Extra: More on LLL and Reducing S-Unit Exponent Bound

For $\psi_h : K \hookrightarrow \mathbb{C}$

$$\Lambda = \sum_{j=0}^{t} a_j \log(\rho_j) = \sum_{j=0}^{t} a_j \kappa_j, \tag{1}$$

where ρ_j are the generators of $\mathcal{O}_S^\times$, $\rho_0 \in \mu_w$.

Extra: More on LLL and Reducing S-Unit Exponent Bound

For $\psi_h : K \hookrightarrow \mathbb{C}$

$$\Lambda = \sum_{j=0}^{t} a_j \log(\rho_j) = \sum_{j=0}^{t} a_j \kappa_j, \qquad (1)$$

where ρ_j are the generators of $\mathcal{O}_S^\times$, $\rho_0 \in \mu_w$.
Choose $C \approx 2^{t/2}$. Define

$$\Phi_0 := \sum_{j=1}^{t} a_j [C\, \Re \kappa_j],$$

$$\Phi_1 := \sum_{j=1}^{t} a_j [C\, \Im \kappa_j] + a_0 [C \cdot \tfrac{2\pi}{w}].$$

so

$$|\Phi_0 + \sqrt{-1}\Phi_i| \leq C|\Lambda| + \frac{1}{\sqrt{2}}(2t+1)K_0$$

since $a_i \leq K_0$ for all i.

Lattice

$$\mathcal{B} := \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ [C\,\Re\kappa_1] & [C\,\Re\kappa_2] & \cdots & [C\,\Re\kappa_{t-1}] & [C\,\Re\kappa_t] & 0 \\ [C\,\Im\kappa_1] & [C\,\Im\kappa_2] & \cdots & [C\,\Im\kappa_{t-1}] & [C\,\Im\kappa_t] & [C\cdot\frac{2\pi}{w}] \end{pmatrix}.$$

Let $\mathcal{L} = L(\mathcal{B}^T)$. Then $\mathbf{a} = (a_1, a_2, \dots, a_{t-1}, \Phi_0, \Phi_1) \in \mathcal{L}$.

Reduction

$$\mathbf{a} = (a_1, a_2, \ldots, a_{t-1}, \Phi_0, \Phi_1) \in \mathcal{L}$$

The Euclidean length of any nonzero lattice element in $\mathcal{L}$ is bounded below by $B := 2^{-t/2}\|\mathbf{b}_1\|$, where $\mathbf{b}_1$ is the shortest vector in the LLL-reduced basis for $\mathcal{L}$.

$$B^2 \leq |\mathbf{a}|^2 = \sum_{i=1}^{t-1} a_i^2 + \Phi_0^2 + \Phi_1^2 \leq C^2|\Lambda|^2 + \frac{1}{2}(2t+1)^2 K_0^2$$

Smart: $|\Lambda| < C_0 e^{-C_1 H}$, by a geometric argument. *holds for some embedding–have to calculate constants for all and take worst constant

$$B^2 \leq C^2(C_0 e^{-C_1 H})^2 + \frac{1}{2}(2t+1)^2 K_0^2$$

Define

$$S_{\mathcal{L}} := \left(B^2 - (t-1)K_0^2\right)^{1/2}, \qquad T_{\mathcal{L}} := \frac{1}{2}\left(w + 2 + \sqrt{2}\right) tK_0.$$

If $B^2 > T_{\mathcal{L}}^2 + (t-1)K_0^2$, then every solution to the S-unit equation satisfies

$$H \leq K_1 := C_6\left(\log(CC_4) - \log(S_{\mathcal{L}} - T_{\mathcal{L}})\right).$$

$$K_1 \sim \log(K_0)$$