Rational Points on Curves

Samir Siksek

Recall: given a curve C over $\mathbb{Q}$, or over a number field k, we want a complete description of $C(k)$. For genus ≥ 1, there is no known algorithm for giving this! But there is a bag of tricks that can be used to show that $C(k)$ is empty, or determine $C(k)$ if it is non-empty. These include:

1. Quotients (lecture 1);
2. Descent (lecture 2);
3. Chabauty (lecture 3);
4. Mordell–Weil sieve (today).

The purpose of these lectures is to get a feel for each of these methods and see it applied to a particular example.

Recap–Jacobians

Associated to a curve C/k of genus $g \geq 1$ is a g-dimensional abelian variety J/k.

(i) For k a number field, $J(k)$ is a finitely generated abelian group (Mordell–Weil Theorem).

(ii) If $C(k) \neq \emptyset$ then $J(k) \cong \mathrm{Pic}^0(C/k)$ (the group of degree 0 rational divisors on C modulo principal divisors).

(iii) If $P_0 \in C(k)$, there is an embedding

$$\iota \ : \ C \hookrightarrow J, \qquad P \mapsto [P - P_0]$$

that is called the Abel–Jacobi map. We have $\iota(C(k)) \subseteq J(k)$.

Recap–Chabauty

Let C be a curve over $\mathbb{Q}_p$ (p is a finite prime). Then there is a pairing

$$\langle\,,\,\rangle \;:\; \Omega_C \times J_C(\mathbb{Q}_p) \to \mathbb{Q}_p,$$

The pairing has the following properties:

1. it is $\mathbb{Q}_p$-linear on the left;
2. it is $\mathbb{Z}$-linear on the right;
3. the kernel on the right is $J(\mathbb{Q}_p)_{\mathrm{tors}}$ (the torsion subgroup of $J(\mathbb{Q}_p)$.

Lemma

Let C be a curve over $\mathbb{Q}$ of genus g. Write r for the rank of $J(\mathbb{Q})$. Suppose $r \leq g-1$. Let p be a prime. Then there is some non-zero $\omega \in \Omega_{C/\mathbb{Q}_p}$ such that

$$\langle \omega, D\rangle = 0 \text{ for all } D \in J(\mathbb{Q}).$$

Proof.

$\dim(\Omega_{C/\mathbb{Q}_p}) = g$. Apply linear algebra. □

We call such ω an **annihilating differential**.

If $P \in C(\mathbb{Q}_p)$ we define the **residue disk of** P by

$$B_p(P) = \{Q \in C(\mathbb{Q}_p) : Q \equiv P \pmod{p}\}.$$

The number of residue disks is $\#C(\mathbb{F}_p)$.
Suppose $r < g - 1$. Let ω be an annihilating differential, and $P \in C(\mathbb{Q})$. Chabauty's method gives a bound $\mathrm{Chab}_p(P)$ for the number of points of rational points in the residue disc of P:

$$\#C(\mathbb{Q}) \cap B_p(P) \leq \mathrm{Chab}_p(P).$$

Let $\mathcal{K}$ be the **known** rational points. If $\#\mathcal{K} \cap B_p(P) = \mathrm{Chab}_p(P)$ then

$$C(\mathbb{Q}) \cap B_p(P) = \mathcal{K} \cap B_p(P).$$

I.e. we know all of the rational points in the residue disc of P.

For Chabauty to succeed in finding $C(\mathbb{Q})$, we need:

1. $r \leq g - 1$;
2. we need explicit generators for $J(\mathbb{Q})$ (or some subgroup of $J(\mathbb{Q})$ of finite index);
3. we want some prime p of good reduction so that the known rational points surject onto $C(\mathbb{F}_p)$;
4. in each residue disc we want to find enough rational points to match the Chabauty bound!

Even if we have (1) and (2), we find in most examples that (3) and (4) fail.

Let

$$C \ : \ y^2 = 2x^6 - 3x^2 - 2x + 1.$$

A short search reveals the following four points:

$$\mathcal{K} = \{(0,1),\ (0,-1),\ (-2,11),\ (-2,-11)\}.$$

Then

$$J(\mathbb{Q}) = \mathbb{Z} \cdot [(-2,-11) - (0,1)]\,.$$

Annhilating differential for $p = 3$ is

$$\omega = (66 + O(3^5))\frac{dx}{y} + \frac{xdx}{y}\,.$$

Applying Chabauty with $p = 3$ we have

P	$\mathrm{Chab}_3(P)$	$\mathcal{K} \cap B_3(P)$
$(0,1)$	2	$\{(0,1)\}$
$(0,-1)$	2	$\{(0,-1)\}$
$(-2,11)$	1	$\{(-2,11)\}$
$(-2,-11)$	1	$\{(-2,-11)\}$

P	$\mathrm{Chab}_3(P)$	$\mathcal{K} \cap B_3(P)$
$(0,1)$	2	$\{(0,1)\}$
$(0,-1)$	2	$\{(0,-1)\}$
$(-2,11)$	1	$\{(-2,11)\}$
$(-2,-11)$	1	$\{(-2,-11)\}$

For $P = (-2,-11)$ and $(-2,11)$ there are no other rational points in the same residue disc. For $P = (0,1)$ and $P = (0,-1)$ we don't know.

Let

$$B_9(P) = \{Q \in C(\mathbb{Q}_3) : Q \equiv P \pmod 9\}.$$

P	$\mathrm{Chab}_9(P)$	$\mathcal{K} \cap B_9(P)$
$(0,1)$	1	$\{(0,1)\}$
$(0,-1)$	1	$\{(0,-1)\}$

For $P = (0,1)$ and $(0,-1)$ there are no other rational points in the smaller residue disc $B_9(P)$.

Note

$$C(\mathbb{F}_3) = \{(\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\}$$

We know all the rational points in

$$B_9(0,1) \cup B_9(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11).$$

This does not fill up $C(\mathbb{Q}_3)$.
To show that $\mathcal{K} = \{(0,1),(0,-1),(-2,11),(-2,-11)\}$ is all of the rational points, we need to show that every rational point belongs to one of these four neighbourhoods. This is what the **Mordell–Weil** sieve will achieve.

Mordell–Weil Sieve

Let $P_0 = (0,1)$. Let

$$\iota \ : \ C \hookrightarrow J, \qquad Q \mapsto [Q - P_0]$$

be the associated Abel-Jacobi map. Recall

$$J(\mathbb{Q}) = \mathbb{Z} \cdot D, \qquad D = [(-2,-11) - (0,1)].$$

Note that

$$\iota(0,1) = 0, \quad \iota(0,-1) = -2D, \quad \iota(-2,11) = -3D, \quad \iota(-2,-11) = D.$$

Suppose $Q \in C(\mathbb{Q})$. Then $\iota(Q) = nD$ with $n \in \mathbb{Z}$. We will use reduction mod p for lots of primes p to 'predict' n.

Suppose $Q \in C(\mathbb{Q})$. Then $\iota(Q) = nD$ with $n \in \mathbb{Z}$. We will use reduction mod p for lots of primes p to 'predict' n.

Let p be a prime of of good reduction. Let

$$N = \text{order of } \bar{D} \in J(\mathbb{F}_p).$$

Consider the commutative diagram

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d, "\mathrm{red}"] & J(\mathbb{Q}) \arrow[d, "\mathrm{red}"] & \mathbb{Z} \arrow[l, "\eta"'] \arrow[d] \\
C(\mathbb{F}_p) \arrow[r, "\iota"] & J(\mathbb{F}_p) & \mathbb{Z}/N\mathbb{Z} \arrow[l, "\eta"']
\end{tikzcd}$$

Here $\eta(m) = mD$. By diagram chasing

$$n \bmod N \in \{m \in \mathbb{Z}/N\mathbb{Z} : m \cdot \bar{D} \in \iota(C(\mathbb{F}_p))\}.$$

Suppose $Q \in C(\mathbb{Q})$. Then $\iota(Q) = nD$ with $n \in \mathbb{Z}$. We will use reduction mod p for lots of primes p to 'predict'n.
For every prime p of good reduction, the Mordell–Weil sieve gives an integer N_p and a set W_p such that $n \bmod N_p \in W_p$.

p	N_p	W_p
3	13	$\{0, 1, 10, 11\}$
5	21	$\{0, 1, 18, 19\}$
7	65	$\{0, 1, 13, 19, 27, 36, 44, 50, 62, 63\}$
23	16	$\{0, 1, 7, 13, 14\}$
61	208	$\{0, 1, 24, 53, 153, 182, 205, 206\}$

Note that $16 \mid 208$.

Suppose $Q \in C(\mathbb{Q})$. Then $\iota(Q) = nD$ with $n \in \mathbb{Z}$. We will use reduction mod p for lots of primes p to 'predict' n.
For every prime p of good reduction, the Mordell–Weil sieve gives an integer N_p and a set W_p such that $n \bmod N_p \in W_p$.

p	N_p	W_p
3	13	$\{0, 1, 10, 11\}$
5	21	$\{0, 1, 18, 19\}$
7	65	$\{0, 1, 13, 19, 27, 36, 44, 50, 62, 63\}$
23	16	$\{0, 1, 7, 13, 14\}$
61	208	$\{0, 1, \cancel{24}, 53, 153, 182, 205, 206\}$

Note that $16 \mid 208$.

Suppose $Q \in C(\mathbb{Q})$. Then $\iota(Q) = nD$ with $n \in \mathbb{Z}$. We will use reduction mod p for lots of primes p to 'predict' n.
For every prime p of good reduction, the Mordell–Weil sieve gives an integer N_p and a set W_p such that $n \bmod N_p \in W_p$.

p	N_p	W_p
3	13	$\{0, 1, 10, 11\}$
5	21	$\{0, 1, 18, 19\}$
7	65	$\{0, 1, 13, 19, 27, 36, 44, 50, 62, 63\}$
23	16	$\{0, 1, 7, 13, 14\}$
61	208	$\{0, 1, \cancel{24, 53, 153, 182,} 205, 206\}$

Note that $13 \mid 65$.

Suppose $Q \in C(\mathbb{Q})$. Then $\iota(Q) = nD$ with $n \in \mathbb{Z}$. We will use reduction mod p for lots of primes p to 'predict' n.
For every prime p of good reduction, the Mordell–Weil sieve gives an integer N_p and a set W_p such that $n \bmod N_p \in W_p$.

p	N_p	W_p
3	13	$\{0, 1, 10, 11\}$
5	21	$\{0, 1, 18, 19\}$
7	65	$\{0, 1, 13, \cancel{19}, 27, 36, \cancel{44}, 50, 62, 63\}$
61	208	$\{0, 1, \cancel{24, 53, 153, 182,} 205, 206\}$

Need more data.

Suppose $Q \in C(\mathbb{Q})$. Then $\iota(Q) = nD$ with $n \in \mathbb{Z}$. We will use reduction mod p for lots of primes p to 'predict' n.
For every prime p of good reduction, the Mordell–Weil sieve gives an integer N_p and a set W_p such that $n \bmod N_p \in W_p$.

p	N_p	W_p
3	13	$\{0, 1, 10, 11\}$
5	21	$\{0, 1, 18, 19\}$
7	65	$\{0, 1, 13, \cancel{19}, 27, 36, \cancel{44}, 50, 62, 63\}$
17	39	$\{0, 1, 36, 37\}$
19	234	$\{0, 1, 42, 67, 72, 82, 100, 132, 150, 160, 165, 190, 231, 232\}$
61	208	$\{0, 1, \cancel{24, 53, 153, 182,} 205, 206\}$

Note that $39 \mid 234$.

Suppose $Q \in C(\mathbb{Q})$. Then $\iota(Q) = nD$ with $n \in \mathbb{Z}$. We will use reduction mod p for lots of primes p to 'predict' n.
For every prime p of good reduction, the Mordell–Weil sieve gives an integer N_p and a set W_p such that $n \bmod N_p \in W_p$.

p	N_p	W_p
3	13	$\{0, 1, 10, 11\}$
5	21	$\{0, 1, 18, 19\}$
7	65	$\{0, 1, 13, \cancel{19}, 27, 36, \cancel{44}, 50, 62, 63\}$
17	39	$\{0, 1, 36, 37\}$
19	234	$\{0, 1, \cancel{42, 67, 72, 82, 100, 132, 150, 160, 165, 190,} 231, 232\}$
61	208	$\{0, 1, \cancel{24, 53, 153, 182,} 205, 206\}$

Note that $39 \mid 234$.

If $Q \in C(\mathbb{Q})$ then $\iota(Q) = nD$ where $n \equiv 0, 1, -3, -2 \pmod{234}$.

But

$$\iota(0,1) = 0, \quad \iota(0,-1) = -2D, \quad \iota(-2,11) = -3D, \quad \iota(-2,-11) = D.$$

Take $n \equiv -3 \pmod{234}$. So $n = -3 + 234m$. Then

$$\begin{aligned} [Q - P_0] &= \iota(Q) = nD \\ &= -3D + m(234 \cdot D) \\ &= \iota(-2,11) + m(234 \cdot D) \\ &= [(-2,11) - P_0] + m(234 \cdot D). \end{aligned}$$

Hence $[Q - (-2,11)] \in m(234 \cdot D)$.

Conclusion: if $Q \in C(\mathbb{Q})$ then $\exists P \in \mathcal{K}$ such that

$$[Q - P] = \mathbb{Z} \cdot (234 \cdot D).$$

p-adic Filtration

Let p be a prime of good reduction. Let

$$J^m(\mathbb{Q}_p) = \{D \in J(\mathbb{Q}_p) : D \equiv 0 \pmod{p^m}\}.$$

We have

$$J(\mathbb{Q}_p) \supset J^1(\mathbb{Q}_p) \supset J^2(\mathbb{Q}_p) \supset J^3(\mathbb{Q}_p) \supset \cdots$$

is a system of decreasing neighbourhoods of the origin. Also

$$J(\mathbb{Q}_p)/J^1(\mathbb{Q}_p) \cong J(\mathbb{F}_p), \qquad J^m(\mathbb{Q}_p)/J^{m+1}(\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^g \text{ for } m \geq 1.$$

For our example,

$$\#J(\mathbb{F}_3) = 13, \qquad 234 = 2 \cdot 3^2 \cdot 13.$$

Hence $234D \in J^3(\mathbb{Q}_3)$. I.e. $234D \equiv 0 \pmod{3^3}$.

End of Example

We have two important pieces of information:

1. If $Q \in C(\mathbb{Q})$ then $\exists P \in \mathcal{K}$ such that
$$[Q - P] \in \mathbb{Z} \cdot (234 \cdot D).$$
2. $234D \equiv 0 \pmod{3^3}$.

Thus
$$Q \equiv P \pmod{3^3}, \qquad P \in \mathcal{K} = \{(0,1), (0,-1), (-2,11), (-2,-11)\}.$$

So Q belongs to
$$\begin{aligned} B_{27}(0,1) \cup B_{27}(0,-1) \cup B_{27}(-2,11) \cup B_{27}(-2,-11) \\ \subset B_9(0,1) \cup B_9(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11). \end{aligned}$$

End of Example

We have two important pieces of information:

1. If $Q \in C(\mathbb{Q})$ then $\exists P \in \mathcal{K}$ such that
$$[Q - P] \in \mathbb{Z} \cdot (234 \cdot D).$$
2. $234D \equiv 0 \pmod{3^3}$.

Thus

$$Q \equiv P \pmod{3^3}, \qquad P \in \mathcal{K} = \{(0,1), (0,-1), (-2,11), (-2,-11)\}.$$

So Q belongs to

$$B_{27}(0,1) \cup B_{27}(0,-1) \cup B_{27}(-2,11) \cup B_{27}(-2,-11)$$
$$\subset B_9(0,1) \cup B_9(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11).$$

Thus (Chabauty and the Mordell–Weil sieve)

$$C(\mathbb{Q}) = \{(0,1),\ (0,-1),\ (-2,11),\ (-2,-11)\}.$$

The Mordell–Weil Sieve

Let $C/\mathbb{Q}$ be a curve, J its Jacobian. Fix $P_0 \in J(\mathbb{Q})$. Let

$$\iota \; : \; C \hookrightarrow J, \qquad P \mapsto [P - P_0]$$

be the Abel–Jacobi map. We assume that we know $J(\mathbb{Q})$ (in other words, we know a basis for $J(\mathbb{Q})$). The **Mordell–Weil Sieve** is a strategy for producing a 'small' finite set $W \subset J(\mathbb{Q})$, and a subgroup $L \subset J(\mathbb{Q})$ of 'huge' index such that

$$\iota(C(\mathbb{Q})) = \bigcup_{D \in W} D + L$$

The Mordell–Weil Sieve

Let $C/\mathbb{Q}$ be a curve, J its Jacobian. Fix $P_0 \in J(\mathbb{Q})$. Let

$$\iota \ : \ C \hookrightarrow J, \qquad P \mapsto [P - P_0]$$

be the Abel–Jacobi map. We assume that we know $J(\mathbb{Q})$ (in other words, we know a basis for $J(\mathbb{Q})$). The **Mordell–Weil Sieve** is a strategy for producing a 'small' finite set $W \subset J(\mathbb{Q})$, and a subgroup $L \subset J(\mathbb{Q})$ of 'huge' index such that

$$\iota(C(\mathbb{Q})) = \bigcup_{D \in W} D + L =: W + L.$$

Inductive Definition

Let $C/\mathbb{Q}$ be a curve, J its Jacobian. Fix $P_0 \in J(\mathbb{Q})$. Let

$$\iota \ : \ C \hookrightarrow J, \qquad P \mapsto [P - P_0]$$

be the Abel–Jacobi map. We define inductively subgroups of finite index $L_i \subset J(\mathbb{Q})$, and finite subsets $W_i \subset J(\mathbb{Q})$, such that

$$L_0 \supseteq L_1 \supseteq L_2 \supseteq L_3 \supset \cdots$$

and

$$\iota(C(\mathbb{Q})) \subset W_i + L_i.$$

Start:

$$L_0 := J(\mathbb{Q}), \qquad W_0 := 0.$$

Inductive Step: choose a prime p of good reduction. Let

$$L_{i+1} = \mathrm{Ker}\left(L_i \hookrightarrow J(\mathbb{Q}) \to J(\mathbb{F}_p)\right).$$

Let

$$W'_{i+1} = W_i + \left(L_i / L_{i+1}\right).$$

Clearly $W'_{i+1} + L_{i+1} = W_i + L_i$. So $\iota(C(\mathbb{Q})) \subset W'_{i+1} + L_{i+1}$.

Consider the commutative diagram

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d, "\mathrm{red}"] & J(\mathbb{Q}) \arrow[d, "\mathrm{red}"] \\
C(\mathbb{F}_p) \arrow[r, "\iota"] & J(\mathbb{F}_p)
\end{tikzcd}$$

Inductive Step: choose a prime p of good reduction. Let

$$L_{i+1} = \operatorname{Ker}\left(L_i \hookrightarrow J(\mathbb{Q}) \to J(\mathbb{F}_p)\right).$$

Let

$$W'_{i+1} = W_i + \left(L_i/L_{i+1}\right).$$

Clearly $W'_{i+1} + L_{i+1} = W_i + L_i$. So $\iota(C(\mathbb{Q})) \subset W'_{i+1} + L_{i+1}$.

Consider the commutative diagram

$$\begin{tikzcd} C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d, "\mathrm{red}"] & W'_{i+1} + L_{i+1} \arrow[d, "\mathrm{red}"] \\ C(\mathbb{F}_p) \arrow[r, "\iota"] & J(\mathbb{F}_p) \end{tikzcd}$$

Inductive Step: choose a prime p of good reduction. Let

$$L_{i+1} = \mathrm{Ker}\left(L_i \hookrightarrow J(\mathbb{Q}) \to J(\mathbb{F}_p)\right).$$

Let

$$W'_{i+1} = W_i + \left(L_i / L_{i+1}\right).$$

Clearly $W'_{i+1} + L_{i+1} = W_i + L_i$. So $\iota(C(\mathbb{Q})) \subset W'_{i+1} + L_{i+1}$.

Consider the commutative diagram

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d, "\mathrm{red}"] & W'_{i+1} + L_{i+1} \arrow[d, "\mathrm{red}"] \arrow[dr] & \\
C(\mathbb{F}_p) \arrow[r, "\iota"] & J(\mathbb{F}_p) & W'_{i+1} \arrow[l, "\mathrm{red}"']
\end{tikzcd}$$

Inductive Step: choose a prime p of good reduction. Let

$$L_{i+1} = \mathrm{Ker}\left(L_i \hookrightarrow J(\mathbb{Q}) \to J(\mathbb{F}_p)\right).$$

Let

$$W'_{i+1} = W_i + \left(L_i/L_{i+1}\right).$$

Clearly $W'_{i+1} + L_{i+1} = W_i + L_i$. So $\iota(C(\mathbb{Q})) \subset W'_{i+1} + L_{i+1}$.

Consider the commutative diagram

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d, "\mathrm{red}"] & W'_{i+1} + L_{i+1} \arrow[d, "\mathrm{red}"] \arrow[dr] & \\
C(\mathbb{F}_p) \arrow[r, "\iota"] & J(\mathbb{F}_p) & W'_{i+1} \arrow[l, "\mathsf{red}"']
\end{tikzcd}$$

Let

$$W_{i+1} = \{w \in W'_{i+1} \ : \ \mathsf{red}(w) \in \iota(C(\mathbb{F}_p))\}.$$

Then $\iota(C(\mathbb{Q})) \subset W_{i+1} + L_{i+1}$.

Choice of p:

1. $[L_i : L_{i+1}]$ is small;
2. $\#J(\mathbb{F}_p)$ is smooth.

In practice, we usually find, **with a good strategy for choosing the p**,

$$W_i = \iota(\mathcal{K}) \qquad (\mathcal{K} \subset C(\mathbb{Q}) \text{ are the known points})$$

for large, and the index $[J(\mathbb{Q}) : L_i]$ is growing slowly.

The L_i are decreasing neighbourhoods of the origin in the profinite topology. When the Mordell–Weil sieve works, it tells us that every rational point on C is close, in the profinite topology on $J(\mathbb{Q})$, to one of the known ones.

Example

$$C \ : \ y^2 - y = x^5 - x, \qquad \iota : C \hookrightarrow J, \ P \mapsto [P - \infty].$$

$$J(\mathbb{Q}) = \mathbb{Z} \cdot D_1 \oplus \mathbb{Z} \cdot D_2 \oplus \mathbb{Z} \cdot D_3,$$

$$D_1 = [(0,1) - \infty], \qquad D_2 = [(1,1) - \infty], \qquad D_3 = [(-1,1) - \infty].$$

The known rational points are

$$\mathcal{K} = \{\infty, \ (-1,0), \ (-1,1), \ (0,0), \ (0,1), \ (1,0), \ (1,1), \ (2,-5), \ (2,6), \ (3,-15), \ (3,16), \ (30,-4929), \ (30,4930), \ (1/4,15/32), \ (1/4,17/32), \ (-15/16,-185/1024), \ (-15/16,1209/1024)\}.$$

Using 922 prime $p < 10^6$ it can be shown that

$$\iota(C(\mathbb{Q})) \subset \iota(\mathcal{K}) + L$$

where

$$[J(\mathbb{Q}) : L] \sim 3.32 \times 10^{3240}.$$

Example

$$C \ : \ y^2 - y = x^5 - x, \qquad \iota : C \hookrightarrow J, \ P \mapsto [P - \infty].$$

The known rational points are

$$\mathcal{K} = \{\infty, \ (-1,0), \ (-1,1), \ (0,0), \ (0,1), \ (1,0), \ (1,1), \ (2,-5), \\ (2,6), \ (3,-15), \ (3,16), \ (30,-4929), \ (30,4930), \ (1/4,15/32), \\ (1/4,17/32), \ (-15/16,-185/1024), \ (-15/16,1209/1024)\}.$$

Using 922 prime $p < 10^6$ it can be shown that

$$\iota(C(\mathbb{Q})) \subset \iota(\mathcal{K}) + L$$

where

$$[J(\mathbb{Q}) : L] \sim 3.32 \times 10^{3240}.$$

The shortest non-zero vector in L has length $\sim 1.156 \times 10^{1080}$. So if $P \in C(\mathbb{Q}) \backslash \mathcal{K}$ then

$$H(P) \geq \exp(10^{2160}).$$

Baker's Bounds

Baker's theory tells us that if P is an **integral point** then

$$H(P) \leq \exp(10^{565}).$$

So we know all the integral points:

$$C(\mathbb{Z}) = \{(-1,0),\ (-1,1),\ (0,0),\ (0,1),\ (1,0),\ (1,1),\ (2,-5),\\ (2,6),\ (3,-15),\ (3,16),\ (30,-4929),\ (30,4930)\}.$$

How do you find the rational points on C?

Baker's Bounds

Baker's theory tells us that if P is an **integral point** then

$$H(P) \leq \exp(10^{565}).$$

So we know all the integral points:

$$C(\mathbb{Z}) = \{(-1,0),\ (-1,1),\ (0,0),\ (0,1),\ (1,0),\ (1,1),\ (2,-5),\ (2,6),\ (3,-15),\ (3,16),\ (30,-4929),\ (30,4930)\}.$$

How do you find the rational points on C?

Thank You!