UNIVERSITÄT BAYREUTH

Descent and Covering Collections Part I: Local Solubility

Michael Stoll
Universität Bayreuth

NATO Advanced Study Institute
Ohrid

September 1, 2014

Hyperelliptic Curves (1)

Let k be a field with $\mathrm{char}(k) \neq 2$.

A **hyperelliptic curve** over k is the smooth projective curve associated to an affine plane curve given by an equation of the form

$$y^2 = f(x) = f_n x^n + f_{n-1} x^{n-1} + \ldots + f_1 x + f_0$$

with $f \in k[x]$ squarefree (i.e., $\mathrm{disc}(f) \neq 0$).

Usually one requires that $\deg(f) \geq 5$.

Hyperelliptic Curves (1)

Let k be a field with $\mathrm{char}(k) \neq 2$.

A **hyperelliptic curve** over k is the smooth projective curve associated to an affine plane curve given by an equation of the form

$$y^2 = f(x) = f_n x^n + f_{n-1} x^{n-1} + \ldots + f_1 x + f_0$$

with $f \in k[x]$ squarefree (i.e., $\mathrm{disc}(f) \neq 0$).

Usually one requires that $\deg(f) \geq 5$.

We write

$$C \colon y^2 = f(x)$$

to denote the projective curve C.

Hyperelliptic Curves (2)

A more abstract definition (that works over any field k) is as follows.

A **hyperelliptic curve** over k is a nice (= smooth, projective and geometrically irreducible) curve C over k with a map $\pi\colon C \to \mathbb{P}^1$ of degree 2, which is defined over k.

Hyperelliptic Curves (2)

A more abstract definition (that works over any field k) is as follows.

A **hyperelliptic curve** over k is a nice (= smooth, projective and geometrically irreducible) curve C over k with a map $\pi\colon C \to \mathbb{P}^1$ of degree 2, which is defined over k.

Writing $k(x)$ for the function field of $\mathbb{P}^1_k$,
the function field of C is a quadratic extension of $k(x)$,
so is of the form $k(x, \sqrt{f(x)})$ if $\mathrm{char}(k) \neq 2$.
Writing y for $\sqrt{f(x)}$, we obtain the equation $\quad y^2 = f(x)$.

Hyperelliptic Curves (2)

A more abstract definition (that works over any field k) is as follows.

A **hyperelliptic curve** over k is a nice (= smooth, projective and geometrically irreducible) curve C over k with a map $\pi\colon C \to \mathbb{P}^1$ of degree 2, which is defined over k.

Writing $k(x)$ for the function field of $\mathbb{P}^1_k$,
the function field of C is a quadratic extension of $k(x)$,
so is of the form $k(x, \sqrt{f(x)})$ if $\mathrm{char}(k) \neq 2$.
Writing y for $\sqrt{f(x)}$, we obtain the equation $y^2 = f(x)$.

In characteristic 2, one has to consider more general equations of the form

$$y^2 + h(x)y = f(x)\,.$$

Hyperelliptic Curves (3)

Let $C\colon y^2 = f(x)$ be a hyperelliptic curve. Then

$$C \text{ has genus } g \iff \deg(f) \in \{2g+1, 2g+2\}.$$

So $\deg(f) \geq 5$ corresponds to $g \geq 2$.

Hyperelliptic Curves (3)

Let $C\colon y^2 = f(x)$ be a hyperelliptic curve. Then

$$C \text{ has genus } g \iff \deg(f) \in \{2g+1, 2g+2\}.$$

So $\deg(f) \geq 5$ corresponds to $g \geq 2$.

A smooth projective model of C can be obtained as follows.
Let $F \in k[x,z]$ be the binary form of degree $2g+2$ such that $F(x,1) = f(x)$.
Then

$$y^2 = F(x,z)$$

defines C as a curve in the weighted projective plane $\mathbb{P}^2_{1,g+1,1}$.

Hyperelliptic Curves (3)

Let $C\colon y^2 = f(x)$ be a hyperelliptic curve. Then

$$C \text{ has genus } g \iff \deg(f) \in \{2g+1, 2g+2\}.$$

So $\deg(f) \geq 5$ corresponds to $g \geq 2$.

A smooth projective model of C can be obtained as follows.
Let $F \in k[x, z]$ be the binary form of degree $2g + 2$ such that $F(x, 1) = f(x)$.
Then

$$y^2 = F(x, z)$$

defines C as a curve in the weighted projective plane $\mathbb{P}^2_{1,g+1,1}$.

So the points at infinity on C are $\infty_s = (1 : s : 0)$ where $s^2 = F(1, 0) = f_{2g+2}$:
There is one point $\infty = \infty_0$ when $\deg(f)$ is odd, otherwise there are two (which are k-rational iff the leading coefficient of f is a square in k).

Hyperelliptic Curves (4)

Any (nice) curve C of genus 2 over k is hyperelliptic over k:

The canonical divisor class has degree 2 and 2-dimensional RR space, so gives rise to a double cover $\pi\colon C \to \mathbb{P}^1$.

Hyperelliptic Curves (4)

Any (nice) curve C of genus 2 over k is hyperelliptic over k:

The canonical divisor class has degree 2 and 2-dimensional RR space, so gives rise to a double cover $\pi\colon C \to \mathbb{P}^1$.

In general, for $g \geq 2$, the moduli space of hyperelliptic curves of genus g has dimension $2g + 3 - \dim \mathrm{GL}(2) = 2g - 1$,
whereas the moduli space of all curves of genus g has dimension $3g - 3$,
so the locus of hyperelliptic curves is of codimension $g - 2$.

Hyperelliptic Curves (4)

Any (nice) curve C of genus 2 over k is hyperelliptic over k:
The canonical divisor class has degree 2 and 2-dimensional RR space,
so gives rise to a double cover $\pi\colon C \to \mathbb{P}^1$.

In general, for $g \geq 2$, the moduli space of hyperelliptic curves of genus g
has dimension $2g + 3 - \dim \mathrm{GL}(2) = 2g - 1$,
whereas the moduli space of all curves of genus g has dimension $3g - 3$,
so the locus of hyperelliptic curves is of codimension $g - 2$.

Since hyperelliptic curves always have the nontrivial automorphism
$\iota\colon (x, y) \mapsto (x, -y)$ (called the 'hyperelliptic involution'),
there can be curves that are non-isomorphic over k,
but become isomorphic over $\bar{k}$.

Rational Points on Hyperelliptic Curves

As usual, we write $C(k)$ for the set of k-rational points on C.

Rational Points on Hyperelliptic Curves

As usual, we write $C(k)$ for the set of k-rational points on C.

We then have for $C\colon y^2 = f(x)$

$$C(k) = \{(\xi,\eta) \in k^2 : \eta^2 = f(\xi)\} \cup \{\infty\} \quad \text{if } \deg(f) \text{ is odd;}$$
$$C(k) = \{(\xi,\eta) \in k^2 : \eta^2 = f(\xi)\} \quad \text{if } \deg(f) \text{ is even and } \operatorname{lcf}(f) \neq \square;$$
$$C(k) = \{(\xi,\eta) \in k^2 : \eta^2 = f(\xi)\} \cup \{\infty_s, \infty_{-s}\} \quad \text{if } \deg(f) \text{ is even and } \operatorname{lcf}(f) = s^2.$$

Rational Points on Hyperelliptic Curves

As usual, we write $C(k)$ for the set of k-rational points on C.

We then have for $C\colon y^2 = f(x)$

$$C(k) = \{(\xi, \eta) \in k^2 : \eta^2 = f(\xi)\} \cup \{\infty\} \qquad \text{if } \deg(f) \text{ is odd;}$$
$$C(k) = \{(\xi, \eta) \in k^2 : \eta^2 = f(\xi)\} \qquad \text{if } \deg(f) \text{ is even and } \operatorname{lcf}(f) \neq \square;$$
$$C(k) = \{(\xi, \eta) \in k^2 : \eta^2 = f(\xi)\} \cup \{\infty_s, \infty_{-s}\} \qquad \text{if } \deg(f) \text{ is even and } \operatorname{lcf}(f) = s^2.$$

In the following, we will concentrate on the case $k = \mathbb{Q}$
(or, more generally, an algebraic number field).

The main question will be:

How can we determine the set $C(\mathbb{Q})$?

General Facts on Rational Points on Curves

Recall the following general classification.

Theorem.

Let C be a (nice) curve over $\mathbb{Q}$ of genus g.

General Facts on Rational Points on Curves

Recall the following general classification.

Theorem.

Let C be a (nice) curve over $\mathbb{Q}$ of genus g.

(1) [classical] If $g = 0$, then $C(\mathbb{Q}) = \emptyset$ or else $C \cong \mathbb{P}^1$ over $\mathbb{Q}$.

General Facts on Rational Points on Curves

Recall the following general classification.

Theorem.

Let C be a (nice) curve over $\mathbb{Q}$ of genus g.

(1) [classical] If $g = 0$, then $C(\mathbb{Q}) = \emptyset$ or else $C \cong \mathbb{P}^1$ over $\mathbb{Q}$.

(2) [Mordell 1922] If $g = 1$, then $C(\mathbb{Q}) = \emptyset$ or else, fixing $P_0 \in C(\mathbb{Q})$, $C(\mathbb{Q})$ is a finitely generated abelian group with zero element P_0 (and (C, P_0) is an elliptic curve over $\mathbb{Q}$).

General Facts on Rational Points on Curves

Recall the following general classification.

Theorem.

Let C be a (nice) curve over $\mathbb{Q}$ of genus g.

(1) [classical] If $g = 0$, then $C(\mathbb{Q}) = \emptyset$ or else $C \cong \mathbb{P}^1$ over $\mathbb{Q}$.

(2) [Mordell 1922] If $g = 1$, then $C(\mathbb{Q}) = \emptyset$ or else, fixing $P_0 \in C(\mathbb{Q})$, $C(\mathbb{Q})$ is a finitely generated abelian group with zero element P_0 (and (C, P_0) is an elliptic curve over $\mathbb{Q}$).

(3) [Faltings 1983] If $g \geq 2$, then $C(\mathbb{Q})$ is finite.

General Facts on Rational Points on Curves

Recall the following general classification.

Theorem.

Let C be a (nice) curve over $\mathbb{Q}$ of genus g.

(1) [classical] If $g = 0$, then $C(\mathbb{Q}) = \emptyset$ or else $C \cong \mathbb{P}^1$ over $\mathbb{Q}$.

(2) [Mordell 1922] If $g = 1$, then $C(\mathbb{Q}) = \emptyset$ or else, fixing $P_0 \in C(\mathbb{Q})$, $C(\mathbb{Q})$ is a finitely generated abelian group with zero element P_0 (and (C, P_0) is an elliptic curve over $\mathbb{Q}$).

(3) [Faltings 1983] If $g \geq 2$, then $C(\mathbb{Q})$ is finite.

Note that this trichotomy is given by the sign (> 0, $= 0$, < 0) of the Euler characteristic $2 - 2g$, which is a topological invariant of the Riemann surface $C(\mathbb{C})$!

Two Problems

We will only consider the case $g \geq 2$.
Then $C(\mathbb{Q})$ is finite and so the points can be enumerated in principle.

Two Problems

We will only consider the case $g \geq 2$.
Then $C(\mathbb{Q})$ is finite and so the points can be enumerated in principle.

However, none of the known proofs of Faltings' Theorem is effective:
It is an open problem whether $C(\mathbb{Q})$ is computable in general.

Two Problems

We will only consider the case $g \geq 2$.
Then $C(\mathbb{Q})$ is finite and so the points can be enumerated in principle.

However, none of the known proofs of Faltings' Theorem is effective:
It is an open problem whether $C(\mathbb{Q})$ is computable in general.

For concrete curves C, we may be able to determine $C(\mathbb{Q})$, though.

Two Problems

We will only consider the case $g \geq 2$.
Then $C(\mathbb{Q})$ is finite and so the points can be enumerated in principle.

However, none of the known proofs of Faltings' Theorem is effective:
It is an open problem whether $C(\mathbb{Q})$ is computable in general.

For concrete curves C, we may be able to determine $C(\mathbb{Q})$, though.

We split the problem into two parts:

(1) Decide whether $C(\mathbb{Q})$ is empty or not!

(2) If $P_0 \in C(\mathbb{Q})$ is given, determine $C(\mathbb{Q})$!

Two Problems

We will only consider the case $g \geq 2$.
Then $C(\mathbb{Q})$ is finite and so the points can be enumerated in principle.

However, none of the known proofs of Faltings' Theorem is effective:
It is an open problem whether $C(\mathbb{Q})$ is computable in general.

For concrete curves C, we may be able to determine $C(\mathbb{Q})$, though.

We split the problem into two parts:

(1) Decide whether $C(\mathbb{Q})$ is empty or not!

(2) If $P_0 \in C(\mathbb{Q})$ is given, determine $C(\mathbb{Q})$!

In this course, we will mainly focus on the first problem.

A Simple Test

Since $\mathbb{Q} \subset \mathbb{R}$, we also have $\mathrm{C}(\mathbb{Q}) \subset \mathrm{C}(\mathbb{R})$,
and we can easily check if $\mathrm{C}(\mathbb{R}) = \emptyset$ or not:

A Simple Test

Since $\mathbb{Q} \subset \mathbb{R}$, we also have $C(\mathbb{Q}) \subset C(\mathbb{R})$,
and we can easily check if $C(\mathbb{R}) = \emptyset$ or not:
if $C\colon y^2 = f(x)$, then $C(\mathbb{R}) = \emptyset$ iff f has no real roots and $\mathrm{lcf}(f) < 0$.

A Simple Test

Since $\mathbb{Q} \subset \mathbb{R}$, we also have $C(\mathbb{Q}) \subset C(\mathbb{R})$,
and we can easily check if $C(\mathbb{R}) = \emptyset$ or not:
if $C\colon y^2 = f(x)$, then $C(\mathbb{R}) = \emptyset$ iff f has no real roots and $\mathrm{lcf}(f) < 0$.

Example.

Let $C\colon y^2 = -x^6 - 17$, then $C(\mathbb{R}) = \emptyset$, whence $C(\mathbb{Q}) = \emptyset$.

A Simple Test

Since $\mathbb{Q} \subset \mathbb{R}$, we also have $C(\mathbb{Q}) \subset C(\mathbb{R})$,
and we can easily check if $C(\mathbb{R}) = \emptyset$ or not:
if $C\colon y^2 = f(x)$, then $C(\mathbb{R}) = \emptyset$ iff f has no real roots and $\mathrm{lcf}(f) < 0$.

Example.

Let $C\colon y^2 = -x^6 - 17$, then $C(\mathbb{R}) = \emptyset$, whence $C(\mathbb{Q}) = \emptyset$.

What about $C\colon y^2 = -x^6 + 3$?

A Simple Test

Since $\mathbb{Q} \subset \mathbb{R}$, we also have $C(\mathbb{Q}) \subset C(\mathbb{R})$,
and we can easily check if $C(\mathbb{R}) = \emptyset$ or not:
if $C\colon y^2 = f(x)$, then $C(\mathbb{R}) = \emptyset$ iff f has no real roots and $\mathrm{lcf}(f) < 0$.

Example.

Let $C\colon y^2 = -x^6 - 17$, then $C(\mathbb{R}) = \emptyset$, whence $C(\mathbb{Q}) = \emptyset$.

What about $C\colon y^2 = -x^6 + 3$?

We have $C(\mathbb{R}) \neq \emptyset$, but we can still prove that $C(\mathbb{Q}) = \emptyset$:

A Simple Test

Since $\mathbb{Q} \subset \mathbb{R}$, we also have $C(\mathbb{Q}) \subset C(\mathbb{R})$,
and we can easily check if $C(\mathbb{R}) = \emptyset$ or not:
if $C\colon y^2 = f(x)$, then $C(\mathbb{R}) = \emptyset$ iff f has no real roots and $\operatorname{lcf}(f) < 0$.

Example.

Let $C\colon y^2 = -x^6 - 17$, then $C(\mathbb{R}) = \emptyset$, whence $C(\mathbb{Q}) = \emptyset$.

What about $C\colon y^2 = -x^6 + 3$?

We have $C(\mathbb{R}) \neq \emptyset$, but we can still prove that $C(\mathbb{Q}) = \emptyset$: Let $\xi \in \mathbb{Q}$.

- If $v_3(\xi) > 0$, then $v_3(-\xi^6 + 3) = 1$, so $-\xi^6 + 3$ cannot be a square;

A Simple Test

Since $\mathbb{Q} \subset \mathbb{R}$, we also have $C(\mathbb{Q}) \subset C(\mathbb{R})$,
and we can easily check if $C(\mathbb{R}) = \emptyset$ or not:
if $C \colon y^2 = f(x)$, then $C(\mathbb{R}) = \emptyset$ iff f has no real roots and $\operatorname{lcf}(f) < 0$.

Example.

Let $C \colon y^2 = -x^6 - 17$, then $C(\mathbb{R}) = \emptyset$, whence $C(\mathbb{Q}) = \emptyset$.

What about $C \colon y^2 = -x^6 + 3$?

We have $C(\mathbb{R}) \neq \emptyset$, but we can still prove that $C(\mathbb{Q}) = \emptyset$: Let $\xi \in \mathbb{Q}$.

- If $v_3(\xi) > 0$, then $v_3(-\xi^6 + 3) = 1$, so $-\xi^6 + 3$ cannot be a square;
- if $v_3(\xi) \leq 0$, then $3^{-6v_3(\xi)}(-\xi^6 + 3) \equiv -1 \bmod 3$; again $-\xi^6 + 3 \neq \square$.

A Simple Test

Since $\mathbb{Q} \subset \mathbb{R}$, we also have $C(\mathbb{Q}) \subset C(\mathbb{R})$,
and we can easily check if $C(\mathbb{R}) = \emptyset$ or not:
if $C\colon y^2 = f(x)$, then $C(\mathbb{R}) = \emptyset$ iff f has no real roots and $\operatorname{lcf}(f) < 0$.

Example.

Let $C\colon y^2 = -x^6 - 17$, then $C(\mathbb{R}) = \emptyset$, whence $C(\mathbb{Q}) = \emptyset$.

What about $C\colon y^2 = -x^6 + 3$?

We have $C(\mathbb{R}) \neq \emptyset$, but we can still prove that $C(\mathbb{Q}) = \emptyset$: Let $\xi \in \mathbb{Q}$.

- If $v_3(\xi) > 0$, then $v_3(-\xi^6 + 3) = 1$, so $-\xi^6 + 3$ cannot be a square;
- if $v_3(\xi) \leq 0$, then $3^{-6v_3(\xi)}(-\xi^6 + 3) \equiv -1 \bmod 3$; again $-\xi^6 + 3 \neq \square$.

Indeed, this proves that $C(\mathbb{Q}_3) = \emptyset$!

$\mathfrak{p}$-adic Numbers (1)

There are two ways of constructing the field $\mathbb{Q}_\mathfrak{p}$ of $\mathfrak{p}$-adic numbers:

$\mathfrak{p}$-adic Numbers (1)

There are two ways of constructing the field $\mathbb{Q}_\mathfrak{p}$ of $\mathfrak{p}$-adic numbers:

- as a completion of $\mathbb{Q}$ (in analogy to $\mathbb{R}$);

p-adic Numbers (1)

There are two ways of constructing the field $\mathbb{Q}_p$ of p-adic numbers:

- as a completion of $\mathbb{Q}$ (in analogy to $\mathbb{R}$);
- as the field of fractions of the projective limit $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

p-adic Numbers (1)

There are two ways of constructing the field $\mathbb{Q}_p$ of p-adic numbers:

- as a completion of $\mathbb{Q}$ (in analogy to $\mathbb{R}$);
- as the field of fractions of the projective limit $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

Define the p-adic absolute value on $\mathbb{Q}$ by

$$|\xi|_p = \begin{cases} 0 & \text{if } \xi = 0; \\ p^{-n} = p^{-v_p(\xi)} & \text{if } \xi = p^n \frac{a}{b} \text{ with } p \nmid ab. \end{cases}$$

p-adic Numbers (1)

There are two ways of constructing the field $\mathbb{Q}_p$ of p-adic numbers:

- as a completion of $\mathbb{Q}$ (in analogy to $\mathbb{R}$);
- as the field of fractions of the projective limit $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

Define the p-adic absolute value on $\mathbb{Q}$ by

$$|\xi|_p = \begin{cases} 0 & \text{if } \xi = 0; \\ p^{-n} = p^{-v_p(\xi)} & \text{if } \xi = p^n \frac{a}{b} \text{ with } p \nmid ab. \end{cases}$$

Then $|\alpha\beta|_p = |\alpha|_p \cdot |\beta|_p$ and $|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\} \leq |\alpha|_p + |\beta|_p$, so we can define $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

p-adic Numbers (1)

There are two ways of constructing the field $\mathbb{Q}_p$ of p-adic numbers:

- as a completion of $\mathbb{Q}$ (in analogy to $\mathbb{R}$);
- as the field of fractions of the projective limit $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

Define the p-adic absolute value on $\mathbb{Q}$ by

$$|\xi|_p = \begin{cases} 0 & \text{if } \xi = 0; \\ p^{-n} = p^{-v_p(\xi)} & \text{if } \xi = p^n \frac{a}{b} \text{ with } p \nmid ab. \end{cases}$$

Then $|\alpha\beta|_p = |\alpha|_p \cdot |\beta|_p$ and $|\alpha + \beta|_p \le \max\{|\alpha|_p, |\beta|_p\} \le |\alpha|_p + |\beta|_p$, so we can define $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

The closed unit ball $\mathbb{Z}_p = \{\xi \in \mathbb{Q}_p : |\xi|_p \le 1\}$ forms a compact subring; it is the topological closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

$\mathfrak{p}$-adic Numbers (2)

It is then easy to check that $p^n\mathbb{Z}_p = \{\xi \in \mathbb{Q}_p : |\xi|_p \leq p^{-n}\}$ and that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

$\mathfrak{p}$-adic Numbers (2)

It is then easy to check that $p^n\mathbb{Z}_p = \left\{\xi \in \mathbb{Q}_p : |\xi|_p \leq p^{-n}\right\}$ and that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

This leads to the description of the ring of p-adic integers as

$$\mathbb{Z}_p = \lim_{\longleftarrow} \mathbb{Z}/p^n\mathbb{Z}\,,$$

which is more suitable for computations.

p-adic Numbers (2)

It is then easy to check that $p^n\mathbb{Z}_p = \left\{\xi \in \mathbb{Q}_p : |\xi|_p \leq p^{-n}\right\}$ and that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

This leads to the description of the ring of p-adic integers as

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}\,,$$

which is more suitable for computations. We then have

$$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Z}_p\left[\tfrac{1}{p}\right]$$

p-adic Numbers (2)

It is then easy to check that $p^n\mathbb{Z}_p = \left\{\xi \in \mathbb{Q}_p : |\xi|_p \le p^{-n}\right\}$ and that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

This leads to the description of the ring of p-adic integers as

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}\,,$$

which is more suitable for computations. We then have

$$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Z}_p\left[\tfrac{1}{p}\right],$$

and we can think of elements of $\mathbb{Q}_p$ as 'Laurent series in p'

$$\xi = \sum_{n=n_0}^{\infty} a_n p^n \qquad \text{with } a_n \in \{0, 1, \ldots, p-1\}.$$

Local Solubility

It can be shown that $\mathbb{R}$ and the $\mathbb{Q}_p$ for all primes p are all the possible completions of $\mathbb{Q}$.

Local Solubility

It can be shown that $\mathbb{R}$ and the $\mathbb{Q}_p$ for all primes p are all the possible completions of $\mathbb{Q}$.

So the following definition makes sense.

Definition.

A (nice) curve C over $\mathbb{Q}$ is said to be everywhere locally soluble or ELS, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

Local Solubility

It can be shown that $\mathbb{R}$ and the $\mathbb{Q}_p$ for all primes p are all the possible completions of $\mathbb{Q}$.

So the following definition makes sense.

Definition.

A (nice) curve C over $\mathbb{Q}$ is said to be everywhere locally soluble or ELS, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

Obviously, $C(\mathbb{Q}) \neq \emptyset$ implies that C is ELS.

Local Solubility

It can be shown that $\mathbb{R}$ and the $\mathbb{Q}_p$ for all primes p are all the possible completions of $\mathbb{Q}$.

So the following definition makes sense.

Definition.

A (nice) curve C over $\mathbb{Q}$ is said to be everywhere locally soluble or ELS, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

Obviously, $C(\mathbb{Q}) \neq \emptyset$ implies that C is ELS.

The converse is true for $g = 0$ ('Hasse Principle')

Local Solubility

It can be shown that $\mathbb{R}$ and the $\mathbb{Q}_p$ for all primes p are all the possible completions of $\mathbb{Q}$.

So the following definition makes sense.

Definition.

A (nice) curve C over $\mathbb{Q}$ is said to be everywhere locally soluble or ELS, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

Obviously, $C(\mathbb{Q}) \neq \emptyset$ implies that C is ELS.

The converse is true for $g = 0$ ('Hasse Principle'), but false in general.

Local Solubility

It can be shown that $\mathbb{R}$ and the $\mathbb{Q}_p$ for all primes p are all the possible completions of $\mathbb{Q}$.

So the following definition makes sense.

Definition.
A (nice) curve C over $\mathbb{Q}$ is said to be everywhere locally soluble or ELS, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

Obviously, $C(\mathbb{Q}) \neq \emptyset$ implies that C is ELS.

The converse is true for $g = 0$ ('Hasse Principle'), but false in general.

Question. Can we decide if a given curve is ELS?

Hensel's Lemma

An important tool for working with $\mathbb{Q}_p$ is provided by Hensel's Lemma:

Hensel's Lemma

An important tool for working with $\mathbb{Q}_p$ is provided by Hensel's Lemma:

Theorem.
Let $f \in \mathbb{Z}_p[x]$ be monic; write $\bar{f}$ for its image in $\mathbb{F}_p[x]$.

Hensel's Lemma

An important tool for working with $\mathbb{Q}_p$ is provided by Hensel's Lemma:

Theorem.
Let $f \in \mathbb{Z}_p[x]$ be monic; write $\bar{f}$ for its image in $\mathbb{F}_p[x]$.
If $a \in \mathbb{F}_p$ such that $\bar{f}(a) = 0$ and $\bar{f}'(a) \neq 0$ (i.e., a is a simple root of $\bar{f}$),

Hensel's Lemma

An important tool for working with $\mathbb{Q}_p$ is provided by Hensel's Lemma:

Theorem.

Let $f \in \mathbb{Z}_p[x]$ be monic; write $\bar{f}$ for its image in $\mathbb{F}_p[x]$.
If $a \in \mathbb{F}_p$ such that $\bar{f}(a) = 0$ and $\bar{f}'(a) \neq 0$ (i.e., a is a simple root of $\bar{f}$),
then there is a unique $\alpha \in \mathbb{Z}_p$ with $\bar{\alpha} = a$ and $f(\alpha) = 0$.

Hensel's Lemma

An important tool for working with $\mathbb{Q}_p$ is provided by Hensel's Lemma:

Theorem.

Let $f \in \mathbb{Z}_p[x]$ be monic; write $\bar{f}$ for its image in $\mathbb{F}_p[x]$.
If $a \in \mathbb{F}_p$ such that $\bar{f}(a) = 0$ and $\bar{f}'(a) \neq 0$ (i.e., a is a simple root of $\bar{f}$),
then there is a unique $\alpha \in \mathbb{Z}_p$ with $\bar{\alpha} = a$ and $f(\alpha) = 0$.

Sketch of proof. Take any α_0 with $\bar{\alpha}_0 = a$ and use Newton iteration. ❑

Hensel's Lemma

An important tool for working with $\mathbb{Q}_p$ is provided by Hensel's Lemma:

Theorem.

Let $f \in \mathbb{Z}_p[x]$ be monic; write $\bar{f}$ for its image in $\mathbb{F}_p[x]$.
If $a \in \mathbb{F}_p$ such that $\bar{f}(a) = 0$ and $\bar{f}'(a) \neq 0$ (i.e., a is a simple root of $\bar{f}$),
then there is a unique $\alpha \in \mathbb{Z}_p$ with $\bar{\alpha} = a$ and $f(\alpha) = 0$.

Sketch of proof. Take any α_0 with $\bar{\alpha}_0 = a$ and use Newton iteration. ❑

Corollary.

Let $\mathcal{C}$ be a curve over $\mathbb{Z}_p$ and let $q \in \mathcal{C}(\mathbb{F}_p)$ be a smooth point on $\mathcal{C} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$.

Hensel's Lemma

An important tool for working with $\mathbb{Q}_p$ is provided by Hensel's Lemma:

Theorem.

Let $f \in \mathbb{Z}_p[x]$ be monic; write $\bar{f}$ for its image in $\mathbb{F}_p[x]$.
If $a \in \mathbb{F}_p$ such that $\bar{f}(a) = 0$ and $\bar{f}'(a) \neq 0$ (i.e., a is a simple root of $\bar{f}$),
then there is a unique $\alpha \in \mathbb{Z}_p$ with $\bar{\alpha} = a$ and $f(\alpha) = 0$.

Sketch of proof. Take any α_0 with $\bar{\alpha}_0 = a$ and use Newton iteration. ❑

Corollary.

Let $\mathcal{C}$ be a curve over $\mathbb{Z}_p$ and let $q \in \mathcal{C}(\mathbb{F}_p)$ be a smooth point on $\mathcal{C} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$.
Then q lifts to a point $Q \in \mathcal{C}(\mathbb{Q}_p)$ (i.e., $\bar{Q} = q$).

Checking for p-adic Points (1)

Theorem (Weil).

Let C be a nice curve of genus g over $\mathbb{F}_p$. Then

$$p + 1 - 2g\sqrt{p} \le \#C(\mathbb{F}_p) \le p + 1 + 2g\sqrt{p}\,.$$

Checking for p-adic Points (1)

Theorem (Weil).

Let C be a nice curve of genus g over $\mathbb{F}_p$. Then

$$p + 1 - 2g\sqrt{p} \le \#C(\mathbb{F}_p) \le p + 1 + 2g\sqrt{p}\,.$$

Corollary.

Let C be a nice curve of genus g over $\mathbb{Q}$,
and let $p \ge 4g^2$ be a prime of good reduction for C.
Then $C(\mathbb{Q}_p) \neq \emptyset$.

Checking for p-adic Points (1)

Theorem (Weil).

Let C be a nice curve of genus g over $\mathbb{F}_p$. Then

$$p + 1 - 2g\sqrt{p} \le \#C(\mathbb{F}_p) \le p + 1 + 2g\sqrt{p}\,.$$

Corollary.

Let C be a nice curve of genus g over $\mathbb{Q}$,
and let $p \ge 4g^2$ be a prime of good reduction for C.
Then $C(\mathbb{Q}_p) \neq \emptyset$.

Proof. Let $\mathcal{C}$ be a model of C over $\mathbb{Z}_p$ with good reduction.

Checking for p-adic Points (1)

Theorem (Weil).

Let C be a nice curve of genus g over $\mathbb{F}_p$. Then

$$p + 1 - 2g\sqrt{p} \le \#C(\mathbb{F}_p) \le p + 1 + 2g\sqrt{p}\,.$$

Corollary.

Let C be a nice curve of genus g over $\mathbb{Q}$,
and let $p \ge 4g^2$ be a prime of good reduction for C.
Then $C(\mathbb{Q}_p) \neq \emptyset$.

Proof. Let $\mathcal{C}$ be a model of C over $\mathbb{Z}_p$ with good reduction.
$p \ge 4g^2$ implies $p \ge 2g\sqrt{p}$, so by Weil, $\mathcal{C}(\mathbb{F}_p) \neq \emptyset$.

Checking for p-adic Points (1)

Theorem (Weil).

Let C be a nice curve of genus g over $\mathbb{F}_p$. Then

$$p + 1 - 2g\sqrt{p} \le \#C(\mathbb{F}_p) \le p + 1 + 2g\sqrt{p}\,.$$

Corollary.

Let C be a nice curve of genus g over $\mathbb{Q}$,
and let $p \ge 4g^2$ be a prime of good reduction for C.
Then $C(\mathbb{Q}_p) \neq \emptyset$.

Proof. Let $\mathcal{C}$ be a model of C over $\mathbb{Z}_p$ with good reduction.
$p \ge 4g^2$ implies $p \ge 2g\sqrt{p}$, so by Weil, $\mathcal{C}(\mathbb{F}_p) \neq \emptyset$.
Every point on $\mathcal{C} \otimes \mathbb{F}_p$ is smooth, so $C(\mathbb{Q}_p) = \mathcal{C}(\mathbb{Q}_p) \neq \emptyset$ by Hensel. ❑

Checking for p-adic Points (2)

If $p < 4g^2$ or the curve has bad reduction at p,
then we still obtain an algorithm for checking if $C(\mathbb{Q}_p) = \emptyset$:

Checking for p-adic Points (2)

If $p < 4g^2$ or the curve has bad reduction at p,
then we still obtain an algorithm for checking if $C(\mathbb{Q}_p) = \emptyset$:

Start with some model $\mathcal{C}$ of C over $\mathbb{Z}_p$.

Checking for p-adic Points (2)

If $p < 4g^2$ or the curve has bad reduction at p,
then we still obtain an algorithm for checking if $C(\mathbb{Q}_p) = \emptyset$:

Start with some model $\mathcal{C}$ of C over $\mathbb{Z}_p$.

- If $\mathcal{C}(\mathbb{F}_p) = \emptyset$, then $C(\mathbb{Q}_p) = \emptyset$.

Checking for p-adic Points (2)

If $p < 4g^2$ or the curve has bad reduction at p,
then we still obtain an algorithm for checking if $C(\mathbb{Q}_p) = \emptyset$:

Start with some model $\mathcal{C}$ of C over $\mathbb{Z}_p$.

- If $\mathcal{C}(\mathbb{F}_p) = \emptyset$, then $C(\mathbb{Q}_p) = \emptyset$.
- If $\mathcal{C}(\mathbb{F}_p)$ contains a smooth point, then $C(\mathbb{Q}_p) \neq \emptyset$.

Checking for p-adic Points (2)

If $p < 4g^2$ or the curve has bad reduction at p,
then we still obtain an algorithm for checking if $C(\mathbb{Q}_p) = \emptyset$:

Start with some model $\mathcal{C}$ of C over $\mathbb{Z}_p$.

- If $\mathcal{C}(\mathbb{F}_p) = \emptyset$, then $C(\mathbb{Q}_p) = \emptyset$.
- If $\mathcal{C}(\mathbb{F}_p)$ contains a smooth point, then $C(\mathbb{Q}_p) \neq \emptyset$.
- Otherwise: for each point $P \in \mathcal{C}(\mathbb{F}_p)$,
  'zoom in' at P to get a new model $\mathcal{C}_P$ and repeat.

Checking for p-adic Points (2)

If $p < 4g^2$ or the curve has bad reduction at p,
then we still obtain an algorithm for checking if $C(\mathbb{Q}_p) = \emptyset$:

Start with some model $\mathcal{C}$ of C over $\mathbb{Z}_p$.

- If $\mathcal{C}(\mathbb{F}_p) = \emptyset$, then $C(\mathbb{Q}_p) = \emptyset$.
- If $\mathcal{C}(\mathbb{F}_p)$ contains a smooth point, then $C(\mathbb{Q}_p) \neq \emptyset$.
- Otherwise: for each point $P \in \mathcal{C}(\mathbb{F}_p)$,
  'zoom in' at P to get a new model $\mathcal{C}_P$ and repeat.
- If for some P, $\mathcal{C}_P(\mathbb{Q}_p) \neq \emptyset$, then $C(\mathbb{Q}_p) \neq \emptyset$, else $C(\mathbb{Q}_p) = \emptyset$.

Checking for p-adic Points (2)

If $p < 4g^2$ or the curve has bad reduction at p,
then we still obtain an algorithm for checking if $C(\mathbb{Q}_p) = \emptyset$:

Start with some model $\mathcal{C}$ of C over $\mathbb{Z}_p$.

- If $\mathcal{C}(\mathbb{F}_p) = \emptyset$, then $C(\mathbb{Q}_p) = \emptyset$.
- If $\mathcal{C}(\mathbb{F}_p)$ contains a smooth point, then $C(\mathbb{Q}_p) \neq \emptyset$.
- Otherwise: for each point $P \in \mathcal{C}(\mathbb{F}_p)$,
  ‘zoom in’ at P to get a new model $\mathcal{C}_P$ and repeat.
- If for some P, $\mathcal{C}_P(\mathbb{Q}_p) \neq \emptyset$, then $C(\mathbb{Q}_p) \neq \emptyset$, else $C(\mathbb{Q}_p) = \emptyset$.

Since we assume that C is smooth,
the ‘zooming in’ will eventually produce models with smooth fiber over $\mathbb{F}_p$.

Deciding Local Solubility

Let

$$C\colon y^2 = f(x)$$

be a hyperelliptic curve of genus g with $f(x) \in \mathbb{Z}[x]$.

Deciding Local Solubility

Let

$$C\colon y^2 = f(x)$$

be a hyperelliptic curve of genus g with $f(x) \in \mathbb{Z}[x]$.

Then

(1) $C(\mathbb{Q}_p) \neq \emptyset$ if $p \geq 4g^2$ and $p \nmid \mathrm{disc}(f)$;

Deciding Local Solubility

Let

$$C\colon y^2 = f(x)$$

be a hyperelliptic curve of genus g with $f(x) \in \mathbb{Z}[x]$.

Then

(1) $C(\mathbb{Q}_p) \neq \emptyset$ if $p \geq 4g^2$ and $p \nmid \mathrm{disc}(f)$;

(2) we can decide if $C(\mathbb{R}) \neq \emptyset$;

Deciding Local Solubility

Let

$$C\colon y^2 = f(x)$$

be a hyperelliptic curve of genus g with $f(x) \in \mathbb{Z}[x]$.

Then

(1) $C(\mathbb{Q}_p) \neq \emptyset$ if $p \geq 4g^2$ and $p \nmid \mathrm{disc}(f)$;

(2) we can decide if $C(\mathbb{R}) \neq \emptyset$;

(3) we can decide if $C(\mathbb{Q}_p) \neq \emptyset$
for the finitely many primes p not covered by (1).

Deciding Local Solubility

Let

$$C\colon y^2 = f(x)$$

be a hyperelliptic curve of genus g with $f(x) \in \mathbb{Z}[x]$.

Then

(1) $C(\mathbb{Q}_p) \neq \emptyset$ if $p \geq 4g^2$ and $p \nmid \mathrm{disc}(f)$;

(2) we can decide if $C(\mathbb{R}) \neq \emptyset$;

(3) we can decide if $C(\mathbb{Q}_p) \neq \emptyset$
for the finitely many primes p not covered by (1).

So we can decide whether C is ELS or not!