Solutions, points, arrows, and paths

Minhyong Kim

November 24, 2006

Solution:

$$(\frac{113259286337279}{449455096000})^2 = (\frac{2340922881}{58675600})^3 - 2$$

Remarkable solution to

$$y^2 = x^3 - 2$$

(say, compared to easy solutions like

$$5^2 = 3^3 - 2)$$

See website of Xavier Xarles

http://mat.uab.es/ xarles/elliptic.html

for instructions on finding such solutions.

Warning: It is *not* a general method.

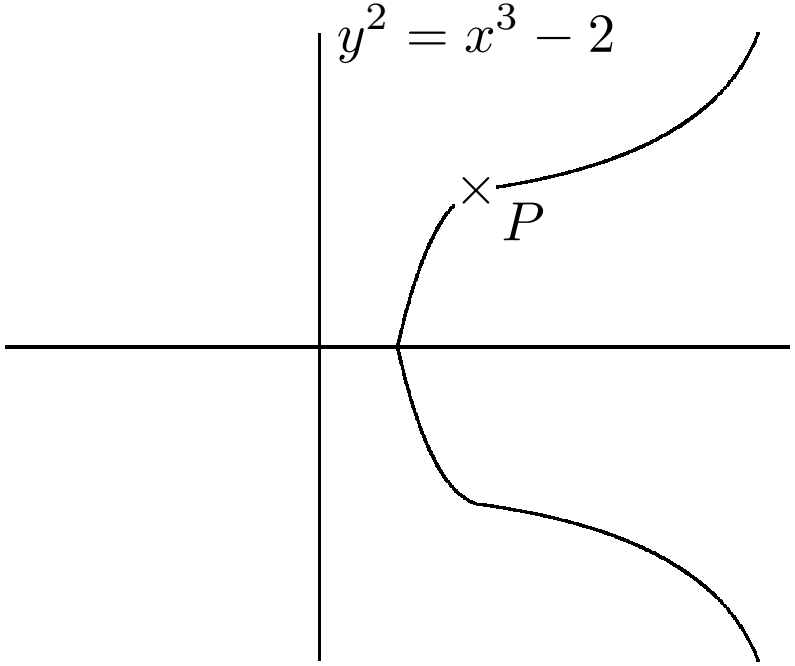
We also say it's a *point*

$$P = (x, y) = (\frac{2340922881}{58675600}, \frac{1132592863372 79}{449455096000})$$

on the algebraic curve

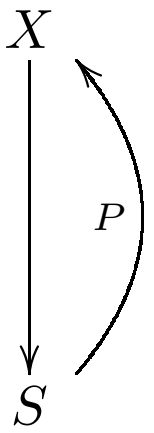
$$y^2 = x^3 - 2$$

Sometimes draw a picture:



View of *classical* algebraic geometry, say à là Weil.

Arrow:



$$S = \mathrm{Spec}(\mathbb{Q})$$

$$X = \mathrm{Spec}(\mathbb{Q}[x, y]/(y^2 - x^3 + 2))$$

This view emphasized by A. Grothendieck.

Can draw another picture by factoring the denominators (the 'poles'). We have

$$449455096000 = 2^6 \cdot 5^3 \cdot 383^3$$

and

$$58675600 = 2^4 \cdot 5^3 \cdot 383^2$$

So solution

$$(\frac{2340922881}{58675600}, \frac{113259286337279}{449455096000})$$

has coordinates in ring

$$\mathbb{Z}[\frac{1}{2 \cdot 5 \cdot 383}]$$

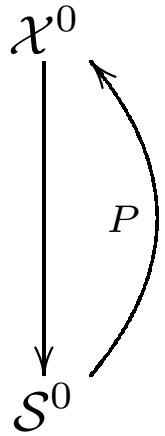
Should think of it as having 'poles' at $(3), (5), (383)$.

Put this fact into visual perspective by introducing the spaces:

$$\mathcal{S}^0 = \mathrm{Spec}(\mathbb{Z}[\frac{1}{2 \cdot 5 \cdot 383}])$$

$$\mathcal{X}^0 = \mathrm{Spec}(\mathbb{Z}[\frac{1}{2 \cdot 5 \cdot 383}][x, y]/(y^2 - x^3 + 2))$$

Then previous diagram of arrows gets refined to

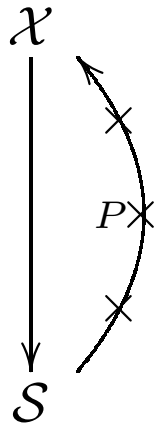


Also, if we put

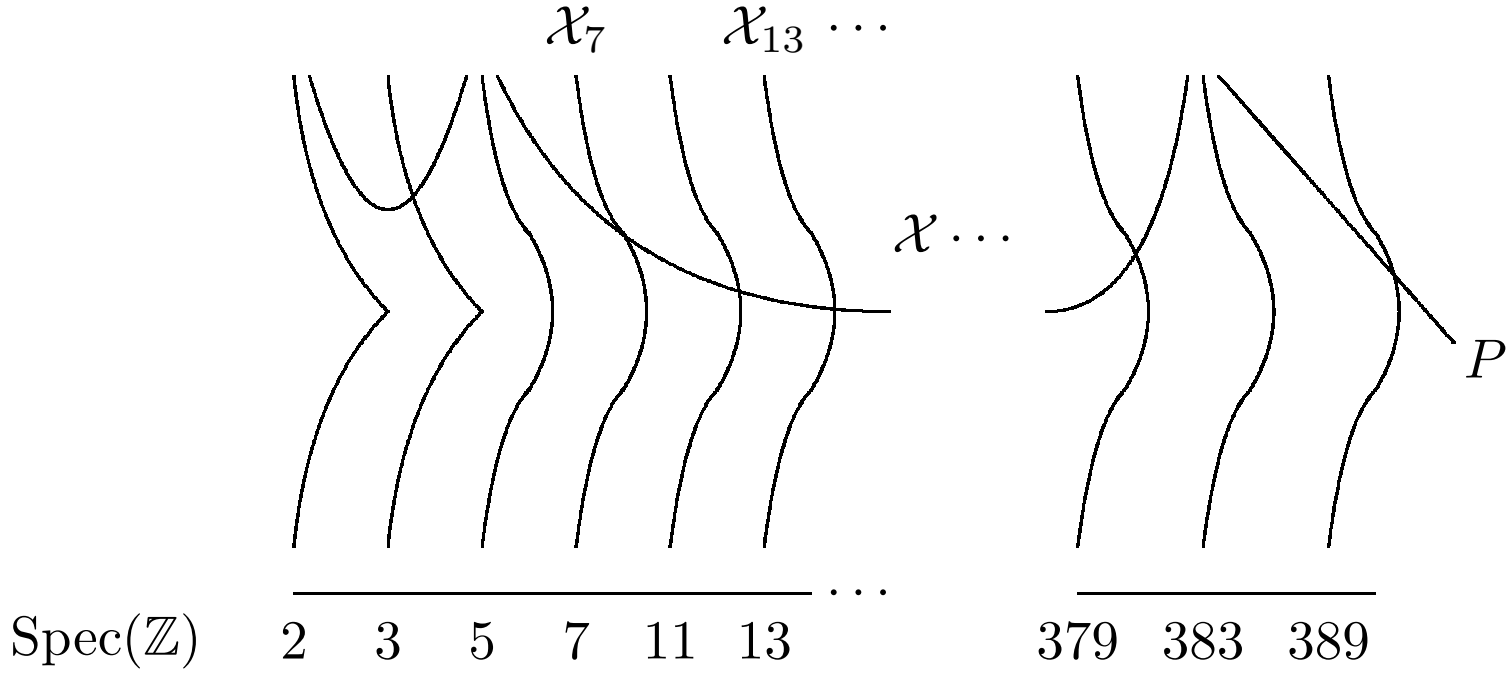
$$\mathcal{S} = \mathrm{Spec}(\mathbb{Z})$$

$$\mathcal{X} = \mathrm{Spec}(\mathbb{Z}[x, y]/(y^2 - x^3 + 2))$$

then picture becomes



Another picture:



Main idea underlying the spatial interpretation of equations and solutions is the

duality between rings and spaces

If X is a (compact) space, it determines a ring $R(X)$ of (continuous) functions.

In many situations, $R(X)$ also determines X. Reason is that X is encoded in $R(X)$ as the set of *maximal ideals*.

$x \in X$ determines

$$m_x := \{h \in R(X) | h(x) = 0\} \subset R(X)$$

and 'all' maximal ideals of R are of this form. That is to say, X can be recovered *purely ring-theoretically* from $R(X)$.

Can also encode maps between spaces.

$$f : X \longrightarrow Y \quad \Rightarrow \quad f^* : R(Y) \longrightarrow R(X)$$

$$f^*(h) = h \circ f$$

In fact, 'any' ring homomorphism is of this form.

Given homomorphism

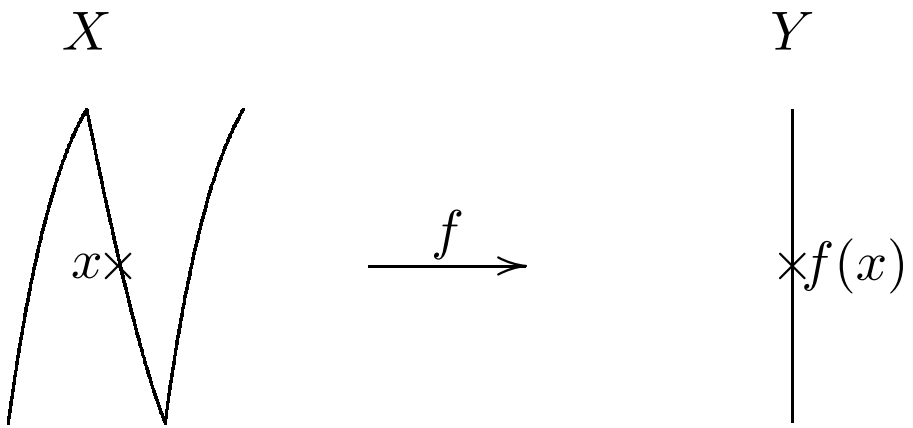
$$\rho : R(Y) \longrightarrow R(X)$$

get map from maximal ideals of $R(X)$ to maximal ideals of $R(Y)$ via

$$\rho^* : m \subset R(X) \mapsto \rho^{-1}(m) \subset R(Y)$$

If $\rho = f^*$ already for some f, can check that $\rho^* = f$, i.e.,

$$(f^*)^* = f$$



$$R(X) \overset{\rho=f^*}{\longleftarrow} R(Y)$$

$$\rho^* : m_x \mapsto m_{f(x)}$$

Surprising implication:

Any commutative ring R with unit can be thought of as a ring of functions on some space

$$\mathrm{Spec}(R)$$

This kind of space is called an *affine scheme*.

Ring homomorphisms can then be thought of as coming from a map of spaces.

$$\rho : A \longrightarrow B \quad \Leftrightarrow \quad \rho^* : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$$

Would like to take the maximal ideals of R as the points of $\mathrm{Spec}(R)$.

But need some more points because of homomorphisms like

$$\rho : \mathbb{Z} \hookrightarrow \mathbb{Q}$$

which should correspond to

$$\rho^* : \mathrm{Spec}(\mathbb{Q}) \rightarrow \mathrm{Spec}(\mathbb{Z})$$

Note, $\rho^*((0)) = \rho^{-1}((0)) = (0)$.

Suffices to take $\mathrm{Spec}(R)$ to be the set of *prime ideals* of R.

Question:

$$A \twoheadrightarrow B$$

What does this mean in terms of

$$\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)?$$

Answer:

$$\mathrm{Spec}(B) \hookrightarrow \mathrm{Spec}(A)$$

If

$$A \twoheadrightarrow B$$

then $B = A/I$ for some ideal I. So if we imagine the *zero set*

$$Z(I) \subset \mathrm{Spec}(A)$$

can interpete B as functions on $Z(I)$.

Example:

$$\mathbb{C}[x,y] \longrightarrow\!\!\!\!\!\rightarrow \mathbb{C}[x]$$

determines an isomorphism

$$\mathbb{C}[x] \simeq \mathbb{C}[x,y]/(y)$$

$\mathbb{C}[x,y]$ functions on

$$\mathbb{C}^2$$

and $\mathbb{C}[x]$ functions on

$$y = 0 \subset \mathbb{C}^2$$

Important special case:

$$f : X \to Y$$

and $y \in Y$, determine the fiber

$$X_y = \{x \in X | f(x) = y\}$$

If $m_y \in R(Y)$ is the maximal ideal determined by y, then it generates an ideal $m_y R(X)$ in $R(X)$ which is exactly the ideal of functions on X that vanish on X_y.

So ring of functions on X_y is

$$R(X)/m_y R(X)$$

In the abstract situation,

$$A \longrightarrow B$$

so that

$$\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$$

and

$$m \subset A$$

is a maximal ideal, then it generates an ideal mB inside B. Then

$$\mathrm{Spec}(B/mB)$$

is the fiber of $\mathrm{Spec}(B)$ over the point $m \in \mathrm{Spec}(A)$.

Example:

$$B = \mathbb{Z}[x, y]/(y^2 - x^3 + 2), \qquad A = \mathbb{Z}$$

So

$$\mathcal{X} = \mathrm{Spec}(B) \to \mathrm{Spec}(\mathbb{Z})$$

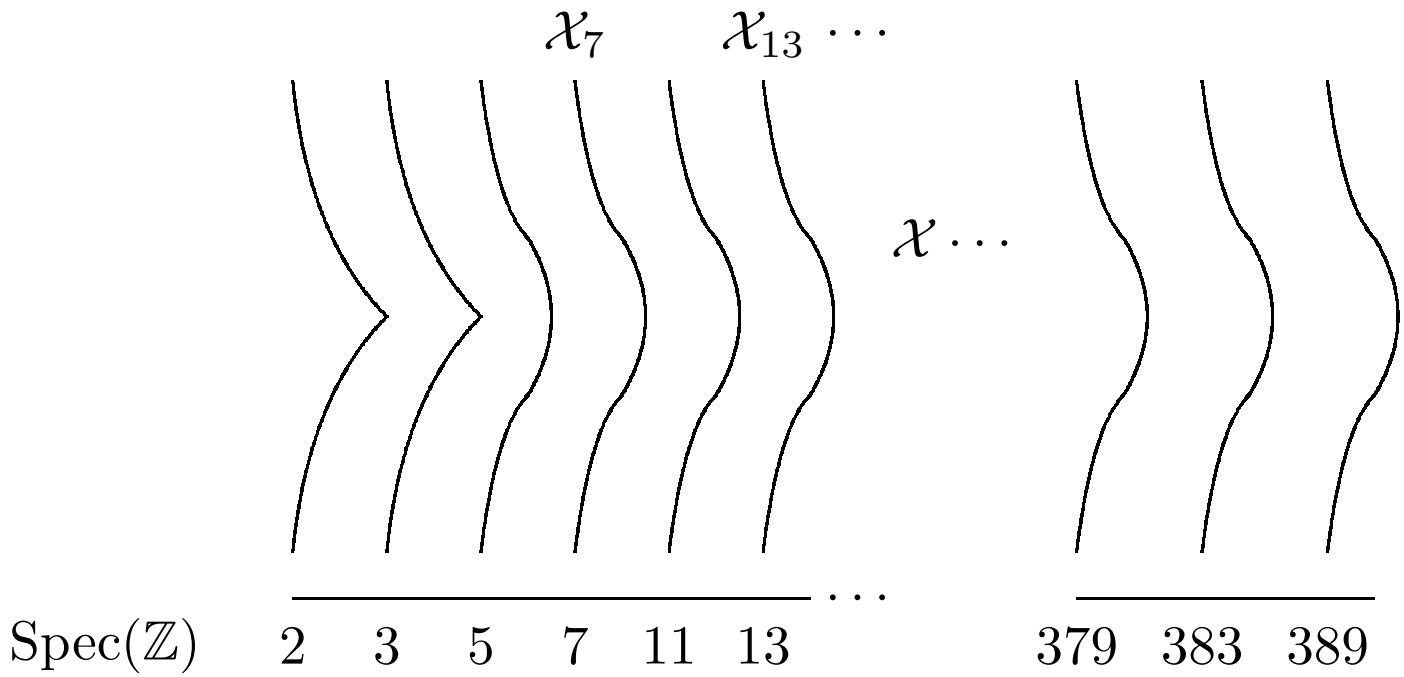
Over the point

$$(7) \in \mathrm{Spec}(\mathbb{Z})$$

we have the fiber of $\mathrm{Spec}(B)$ over (7)

$$\mathrm{Spec}(\mathbb{F}_7[x, y]/(y^2 - x^3 + 2))$$

That is, the fibers are *curves over finite fields.*


$\mathcal{X}_7$
$\mathcal{X}_{13}$ $\cdots$
$\mathcal{X}$ $\cdots$
$\cdots$
Spec($\mathbb{Z}$)
2 3 5 7 11 13
379 383 389

A ring and $f(x,y) \in A[x,y]$.

$$B = A[x,y]/(f(x,y))$$

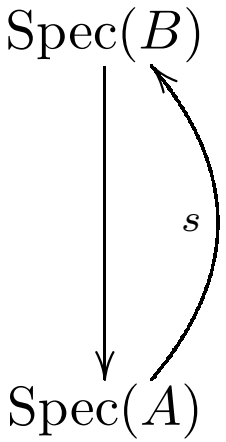
Then there is a natural homomorphism

$$g^* : A \to B$$

So we have a map

$$g : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

What are the sections of g



i.e., the maps $s : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ such that $g \circ s = Id$?

Should be in correspondence with $s^* : B \rightarrow A$ such that

$$s^* \circ g^* = Id$$

Since $B = A[x, y]/(f(x, y))$, s^* is completely determined by

$$a_1 = s^*(x), \quad a_2 = s^*(y)$$

That is, must have

$$s^*(h(x,y)) = h(a_1, a_2)$$

Note that *any* assignment of a_1 and a_2 determines a ring homomorphism

$$A[x,y] \to A$$

When does such an assignment determine a homomorphism

$$A[x,y]/(f(x,y)) \to A?$$

Exactly when $f(a_1, a_2) = 0$.

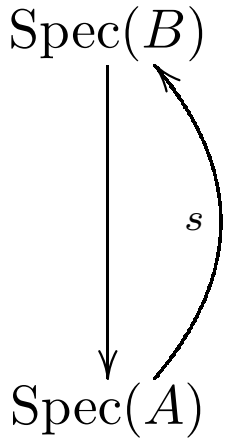
That is, s are in correspondence with the *solutions* in A of

$$f(x, y) = 0$$

To reverse the viewpoint, solutions of

$$f(x, y) = 0$$

in A are in 1-1 correspondence with diagrams



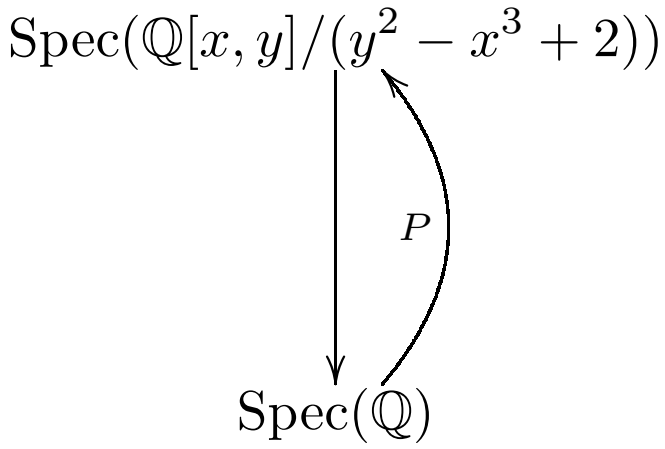
Go back to

$$\mathrm{Spec}(\mathbb{Q}[x,y]/(y^2-x^3+2))\to\mathrm{Spec}(\mathbb{Q})$$

The solution

$$P=(x,y)=(\frac{2340922881}{58675600},\frac{113259286337279}{449455096000})$$

corresponds to one such diagram



We can also consider

$$\mathrm{Spec}(\mathbb{Z}[x,y]/(y^2-x^3+2))\to\mathrm{Spec}(\mathbb{Z})$$

But P is *not* a section for this arrow because

$$P^*(x)=\frac{2340922881}{58675600}$$

and

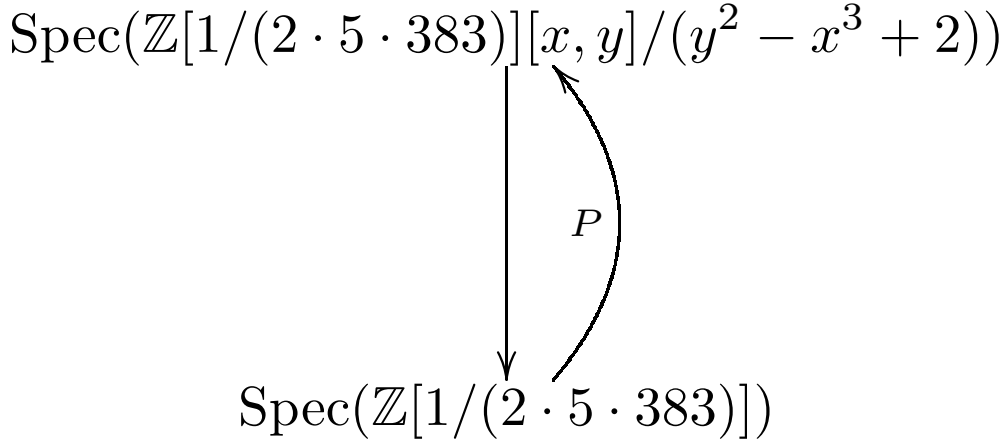
$$P^*(y)=\frac{113259286337279}{449455096000}$$

are not in $\mathbb{Z}$.

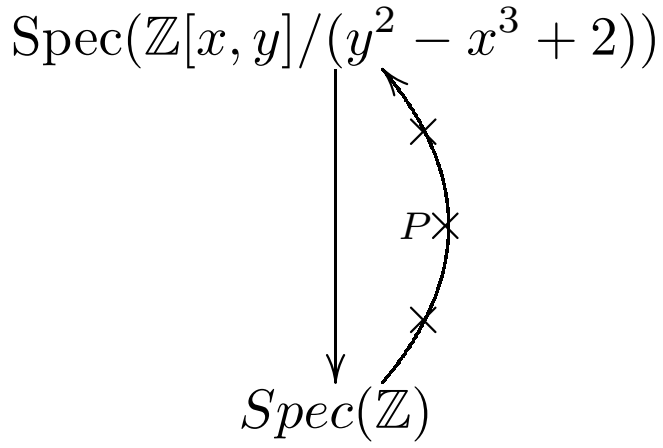
However, if we consider

$$\mathrm{Spec}(\mathbb{Z}[1/(2\cdot 5\cdot 383)][x,y])/(y^2-x^3+2))\to\mathrm{Spec}(\mathbb{Z}[1/(2\cdot 5\cdot 383)])$$

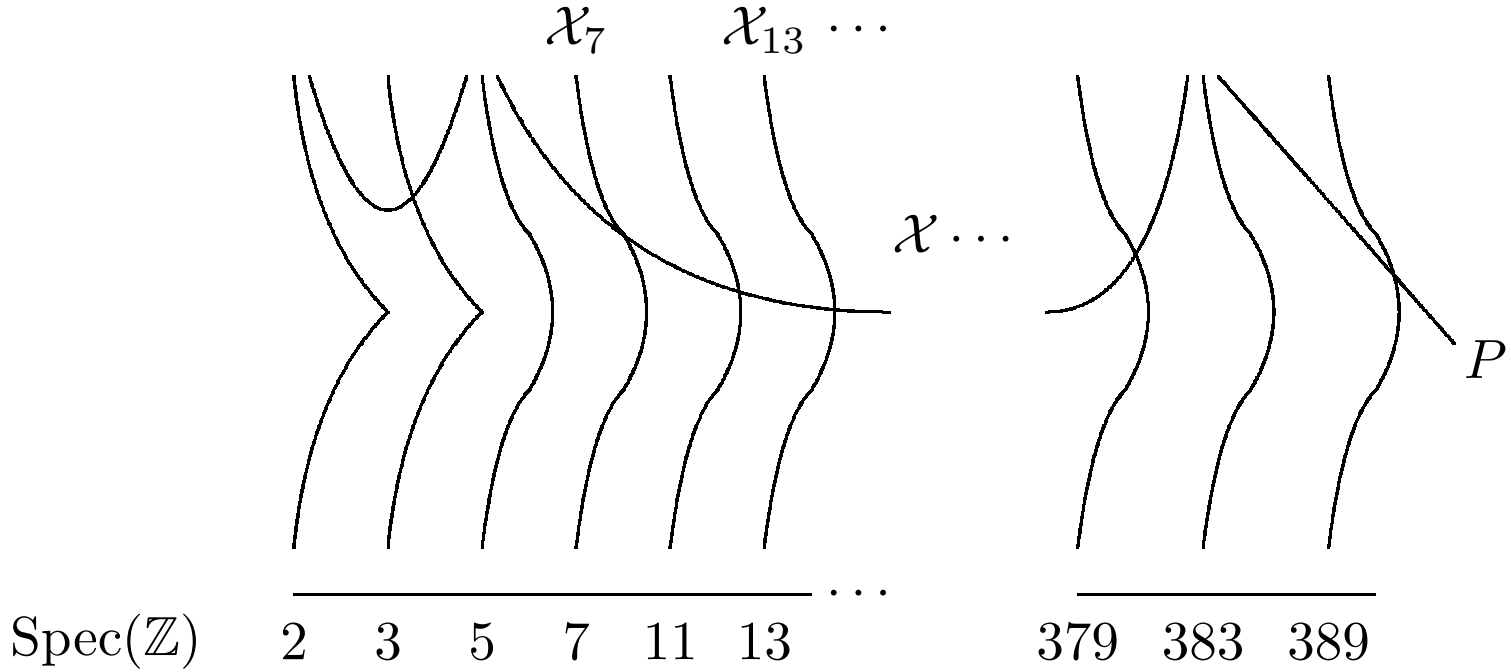
P does define



Also view this using another picture from the beginning



the notation indicating that P is *not defined everywhere.* (It is defined on a dense open set.)


$\mathcal{X}_7$
$\mathcal{X}_{13}$ $\cdots$
$\mathcal{X}$ $\cdots$
P
$\cdots$
Spec($\mathbb{Z}$)
2 3 5 7 11 13
379 383 389

The ‘arrow-theoretic’ interpretation of solutions to equations is the beginning of arithmetic geometry.

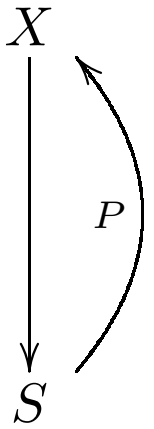
Grothendieck:

> In our acquisition of knowledge of the Universe (whether mathematical or otherwise) that which renovates the quest is nothing more nor less than complete innocence. It is in this state of complete innocence that we receive everything from the moment of our birth. Although so often the object of our contempt and of our private fears, it is always in us. It alone can unite humility with boldness so as to allow us to penetrate to the heart of things, or allow things to enter us and taken possession of us.
>
> This unique power is in no way a privilege given to "exceptional talents" - persons of incredible brain power (for example), who are better able to manipulate, with dexterity and ease, an enormous mass of data, ideas and specialized skills. Such gifts are undeniably valuable, and certainly worthy of envy from those who (like myself) were

not so "endowed at birth, far beyond the ordinary".

Yet it is not these gifts, nor the most determined ambition combined with irresistible will-power, that enables one to surmount the "invisible yet formidable boundaries" that encircle our universe. Only innocence can surmount them, which mere knowledge doesn't even take into account, in those moments when we find ourselves able to listen to things, totally and intensely absorbed in child's play.

For Grothendieck, the diagram

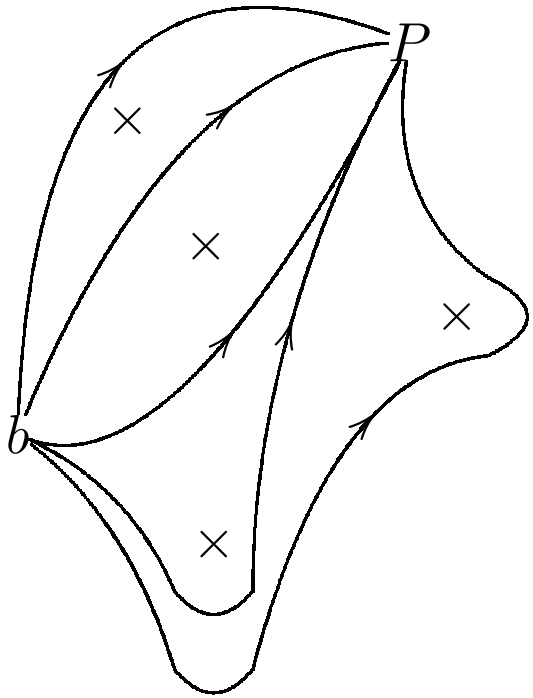


is considerably more innocent than the equation

$$(\frac{113259286337279}{449455096000})^2 = (\frac{2340922881}{58675600})^3 - 2$$

if one views the former as a *primary object* rather than as a *macro* for the latter.

Finally, *paths*



To explain, return for a moment to the 'concrete' view of the equation

$$y^2 = x^3 - 2$$

If we look at the *complex* solutions, it forms a nice topological space

$$X^{top}$$

a torus with one point removed.

Choose a point $b \in X$, say $b = (3, 5)$.

We then have the fundamental group

$$\pi_1(X^{top}, b)$$

consisting of homotopy classes of loops based at b.

Also consider

$$\pi_1(X^{top}; b, x)$$

consisting of homotopy classes of paths from b to x.

We now wish to encode any point x into the set

$$\pi_1(X^{top}; b, x)$$

It is a well-established practice to replace points by objects with more structure in order to *magnify* their properties.

Perhaps best known example:

$$a^n + b^n = c^n \Leftrightarrow y^2 = x(x - a^n)x + b^n$$

$$x \mapsto \pi_1(X^{top}; b, x)$$

describes such a procedure of an *extremely canonical sort*.

But how could this be useful since

$$\pi_1(X^{top}; b, x)$$

are all the same for different x?

Important point: They are not *canonically* the same.

Thus, when endowed with natural extra structure, can often genuinely distinguish them from each other.

Most important extra structure is a *Galois action.*

$$\Gamma := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

Then Γ 'almost' acts on $\pi_1(X^{top}, b)$ and all the $\pi_1(X^{top}; b, x)$ as x runs through rational solutions.

Actual action is on the compatible systems

$$(\gamma_H)_H$$

where H runs through subgroups of $\pi_1(X^{top}, b)$ of finite index and

$$\gamma_H \in \pi_1(X^{top}, b)/H$$

Here, compatibility is with respect to the natural maps

$$\pi_1(X^{top}, b)/H \to \pi_1(X^{top}, b)/H'$$

whenever $H \subset H'$. The collection of such (γ_H) is called the *pro-finite completion* of $\pi_1(X^{top}, b)$ and denoted

$$\hat{\pi}_1(X^{top}, b)$$

Similarly, can form pro-finite completions

$$\hat{\pi}_1(X^{top}; b, x)$$

To do this, note that $\pi_1(X^{top}, b)$ acts simply transitively on $\pi_1(X^{top}; b, x)$ on the right:

$$(p, \gamma) \mapsto p \circ \gamma$$

We say $\pi_1(X^{top}; b, x)$ is a right $\pi_1(X^{top}, b)$-torsor.

Then consider compatible systems

$$(p_H)_H$$

for

$$p_H \in \pi_1(X^{top}; b, x)/H$$

as H runs through subgroups of $\pi_1(X^{top}, b)$ of finite index. The collection of such make up

$$\hat{\pi}_1(X^{top}; b, x)$$

This is a right $\hat{\pi}_1(X^{top}, b)$-torsor.

Fact, $\hat{\pi}_1(X^{top}, b)$ and all the

$$\hat{\pi}_1(X^{top}; b, x)$$

admit compatible actions of Γ.

We will describe one relatively explicit realization to describe this action.

We need to use an algebraic counterpart of the *universal covering space*

$$\tilde{X}$$

of X. In fact, in topology, the set $\tilde{X}$ can be simply *constructed* as

$$\cup_x \pi_1(X^{top}; b, x)$$

and then topologized suitably. In fact, given any other construction $\tilde{X}'$, a choice $b' \in \tilde{X}'$ will determine a bijection

$$\cup_x \pi_1(X^{top}; b, x) \simeq \tilde{X}'$$

via canonical lifting of paths.

In this construction, the map

$$\tilde{X} \longrightarrow\!\!\!\!\!\rightarrow X$$

simply sends a path $p \in \pi_1(X; b, x)$ to its endpoint x. In particular, we get an identification of the fiber

$$\tilde{X}_x \simeq \pi_1(X^{top}; b, x)$$

Construction of an algebraic $\tilde{X}$ gives us an entirely analogous interpretation of

$$\hat{\pi}_1(X^{top}; b, x)$$

Simple example of $\mathbb{C}^*$. This is the algebraic curve

$$Z := \mathbb{C}[x, y]/(xy - 1)$$

and hence, can be view as the complex points of

$$\mathrm{Spec}(\mathbb{Q}[x, y]/(xy - 1))$$

Usual universal covering is

$$\mathbb{C} \xrightarrow{\exp} \mathbb{C}^*$$

Algebraic counterpart is the system

$$\{\mathbb{C}^* \xrightarrow{z^n} \mathbb{C}^*\} \longrightarrow \mathbb{C}^*$$

One arrives at a canonical identification

$$\hat{\pi}_1(Z,1) \simeq \{\mathbb{C}^* \xrightarrow{z^n} \mathbb{C}^*\}_1$$

$$\simeq \{\text{compatible collections of roots of unity}\}$$

Similarly, for any rational point $x \in \mathbb{C}^*$, we get

$$\hat{\pi}_1(Z;1,x) \simeq \{\mathbb{C}^* \xrightarrow{z^n} \mathbb{C}^*\}_x$$

$$\simeq \{\text{compatible collections of roots of } x\}$$

In particular, we see the Γ-action.

Notice that

$$\{\text{compatible collections of roots of unity}\}$$

$$\simeq \{\text{compatible collections of roots of } x\}$$

as sets, but *not* in a way compatible with Γ action. Thus, in the category of sets with Γ action, they are genuinely distinct. Can show similarly that

$$\hat{\pi}_1(Z; 1, x) \neq \hat{\pi}_1(Z; 1, y)$$

as right $\hat{\pi}_1(X^{top}, b)$-torsors with Γ action if $x \neq y$. Proof requires a version of the Dirichlet unit theorem.

More generally, if X is any smooth algebraic curve defined over $\mathbb{Q}$ which is not simply connected and $b \in X(\mathbb{Q})$ is a rational point, then

$$\hat{\pi}_1(X^{top}; b, x) \simeq \hat{\pi}_1(X^{top}; b, y)$$

as right $\hat{\pi}_1(X^{top}, b)$-torsors with Γ-action if $x \neq y$. Uses the Mordell-Weil theorem.

Starting point of

Anabelian Diophantine geometry

Remarks:

-Term ‘anabelian’ coined by Grothendieck in the 80’s.

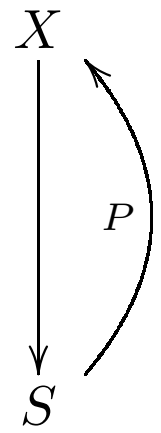
-Arithmetic theory of fundamental group goes back to 60’s, but Diophantine considerations in this context begins with a letter from Grothendieck to Faltings in the 80’s.

-Very speculative version of such ideas proposed by André Weil in 30’s.

‘Poetry begins to atrophy when it strays too far from music. Music begins to atrophy when it strays too far from dance.’

-Ezra Pound.

$$f(x_1, x_2) = 0$$


X
P
S