Solving Problems With Topos Theory:

The Weil Conjectures

Chris Grossack
(they/them)

NB:

NB:

↳ I'm an idiot at the best of times

NB:

↳ I'm an idiot at the best of times

↳ I'm <u>not</u> an expert, or even particularly well informed on this topic.

NB:

↳ I'm an idiot at the best of times

↳ I'm <u>not</u> an expert, or even particularly well informed on this topic.

↳ that said, I'm a <u>well read</u> idiot, and this talk is an amalgamation of other talks by actual experts.

In particular, you should look into

$\boxed{\mathrm{I}}$ The Weil Conjectures, from Abel to Deligne (Sophie Morel)

$\boxed{\mathrm{II}}$ Nevertheless, one should learn the language of topos (Colin McLarty)

In particular, you should look into

$\boxed{\text{I}}$ The Weil Conjectures, from Abel to Deligne (Sophie Morel)

$\boxed{\text{II}}$ Nevertheless, one should learn the language of topos (Colin McLarty)

↳ both are on youtube.

These slides will also be on my blog at

grossack.site

These slides will also be on my blog at

grossack.site

↳ that page will also have the paper associated to this talk

These slides will also be on my blog at

grossack.site

↳ that page will also have the paper associated to this talk

↳ obviously <u>no</u> ideas are my own! see the paper for references.

On with the show!

§1

What <u>Are</u> the Weil Conjectures?

Let's look at a concrete problem.

Let's look at a <u>concrete problem</u>.

<u>Q</u> how many solutions to

$$x^2 + y^2 = 1$$

in the finite field $\mathbb{F}_{p^n}$?

When in doubt, ask a computer:

When in doubt, ask a computer:

	p^1	p^2	p^3	p^4	p^5
$p=2$	2	4	8	16	32
$p=3$	4	8	28	80	244
$p=5$	4	24	124	624	3124
$p=7$	8	48	344	2400	16808
$p=11$	12	120	1332	14640	161052

	p^1	p^2	p^3	p^4	p^5
$p=2$	2	4	8	16	32
$p=3$	4	8	28	80	244
$p=5$	4	24	124	624	3124
$p=7$	8	48	344	2400	16808
$p=11$	12	120	1332	14640	161052

obvious pattern!

$\hookrightarrow N(2^k) = 2^k$

	p^1	p^2	p^3	p^4	p^5
$p=2$	2	4	8	16	32
$p=3$	4	8	28	80	244
$p=5$	4	24	124	624	3124
$p=7$	8	48	344	2400	16808
$p=11$	12	120	1332	14640	161052

obvious pattern!

$\hookrightarrow N(2^k) = 2^k$

$\hookrightarrow N(p^k) = p^k \pm 1$

	p^1	p^2	p^3	p^4	p^5
$p = 2$	2	4	8	16	32
$p = 3$	4	8	28	80	244
$p = 5$	4	24	124	624	3124
$p = 7$	8	48	344	2400	16808
$p = 11$	12	120	1332	14640	161052

obvious pattern!

↳ $N(2^k) = 2^k$

↳ $N(p^k) = p^k \pm 1$

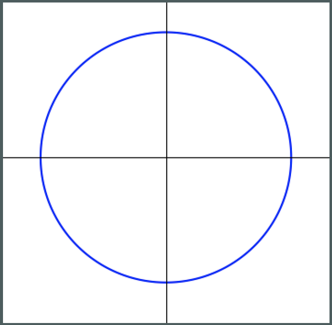
↳ ... why?

A Geometry!

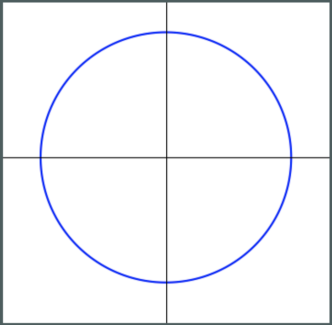
A

Geometry!

↳ $x^2+y^2=1$ ⇝

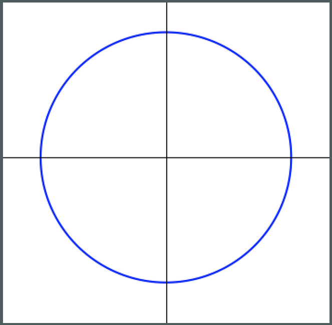


$\underline{A}$ Geometry!

↳ $x^2+y^2=1$ ⟶ 

↳ this is $\underline{1}$-dimensional.

A Geometry!

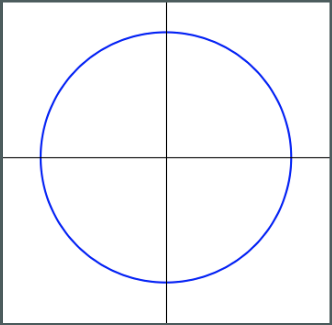
↳ $x^2 + y^2 = 1 \rightsquigarrow$ 

↳ this is $\underline{1}$-dimensional.

↳ so we expect $\{x^2+y^2=1\} \approx \mathbb{A}^1$

$\underline{A}$ Geometry!

$\hookrightarrow x^2+y^2=1 \rightsquigarrow$



$\hookrightarrow$ this is $\underline{1}$-dimensional.

"affine line"

$\hookrightarrow$ so we expect $\{x^2+y^2=1\} \approx \mathbb{A}^1$

In fact:

$$\left|\{(x,y)\in \mathbb{F}_{p^n} \mid x^2+y^2=1\}\right| = \left|\mathbb{A}^1_{\mathbb{F}_{p^n}}\right| \pm \text{error}$$

In fact:

$$\left|\left\{(x,y)\in\mathbb{F}_{p^n} \mid x^2+y^2=1\right\}\right| = \left|\mathbb{A}^1_{\mathbb{F}_{p^n}}\right| \pm \text{error}$$

p^n

In fact:

$$\left|\{(x,y)\in\mathbb{F}_{p^n} \mid x^2+y^2=1\}\right| = \left|\mathbb{A}^1_{\mathbb{F}_{p^n}}\right| \pm \text{error}$$

$$\uparrow p^n$$

More generally, if $\dim(X)=d$,

$$\left|X(\mathbb{F}_{p^n})\right| = \left|\mathbb{A}^d_{\mathbb{F}_{p^n}}\right| \pm \text{error}$$

In fact:

$$\left|\left\{(x,y)\in\mathbb{F}_{p^n} \mid x^2+y^2=1\right\}\right| = \left|\underbrace{\mathbb{A}^1_{\mathbb{F}_{p^n}}}_{p^n}\right| \pm \text{error}$$

More generally, if $\dim(X)=d$,

$$\left|X(\mathbb{F}_{p^n})\right| = \left|\underbrace{\mathbb{A}^d_{\mathbb{F}_{p^n}}}_{(p^n)^d}\right| \pm \text{error}$$

The Weil Conjectures are about controlling this error term!

The Weil Conjectures are about controlling this error term!

↳ let's introduce some notation.

§2

Some Notation

$\underline{\text{Def}^{\underline{n}}}$

Let $X = \{f_\alpha\}$ be a family of polynomials in $\mathbb{Z}[x_1 \cdots x_n]$

$\underline{Def^{\underline{n}}}$

Let $X = \{f_\alpha\}$ be a family of polynomials in $\mathbb{Z}[x_1 \cdots x_n]$

Let k be a field

$\underline{\text{Def}^{\underline{n}}}$

Let $X = \{f_\alpha\}$ be a family of polynomials in $\mathbb{Z}[x_1 \cdots x_n]$

Let k be a field

we write $X(k)$ for

$$\{\bar{x} \in k^n \mid \forall \alpha.\ f_\alpha(\bar{x}) = 0\}$$

eg let $\mathcal{C} = \{x^2 + y^2 - 1\}$.

eg let $\mathcal{C} = \{x^2 + y^2 - 1\}$.

then $\mathcal{C}(\mathbb{R})$ is the unit circle

eg let $\mathcal{C} = \{x^2 + y^2 - 1\}$.

then $\cdot\ \mathcal{C}(\mathbb{R})$ is the unit circle

$\cdot\ \mathcal{C}(\mathbb{Q})$ are <u>rational</u> points on the unit circle eg let $\mathcal{C} = \{x^2+y^2-1\}$.

then
- $\mathcal{C}(\mathbb{R})$ is the unit circle
- $\mathcal{C}(\mathbb{Q})$ are rational points on the unit circle
- We want to count $\mathcal{C}(\mathbb{F}_{p^n})$.

These are <u>Affine Schemes</u>

and are <u>very</u> natural algebraically.

These are <u>Affine Schemes</u>

and are <u>very</u> natural algebraically.

↳ unfortunately, they're <u>less</u> natural geometrically...

These are <u>Affine Schemes</u>

and are <u>very</u> natural algebraically.

↳ unfortunately, they're <u>less</u> natural geometrically...

↳ they're "missing points", which makes counting problems less elegant.

Defn

Let $X = \{f_\alpha\}$ be a family of <u>homogeneous</u> polynomials in $\mathbb{Z}[x_0 \dots x_n]$

Def^n

Let $X = \{f_\alpha\}$ be a family of homogeneous polynomials in $\mathbb{Z}[x_0 \dots x_n]$

$f(\lambda \cdot \bar{x}) = \lambda^d \cdot f(\bar{x})$

Def^n

Let $X = \{f_\alpha\}$ be a family of homogeneous polynomials in $\mathbb{Z}[x_0 \cdots x_n]$

$$f(\lambda \cdot \bar{x}) = \lambda^d \cdot f(\bar{x})$$

Then we write

$$X(k) = \left\{ \bar{x} \in k^{n+1} \setminus \{\bar{0}\} \;\middle|\; \forall \alpha.\, f_\alpha(\bar{x}) = 0 \right\} \Big/ \begin{smallmatrix} \bar{x} = \lambda \bar{x} \\ \forall \lambda \neq 0. \end{smallmatrix}$$

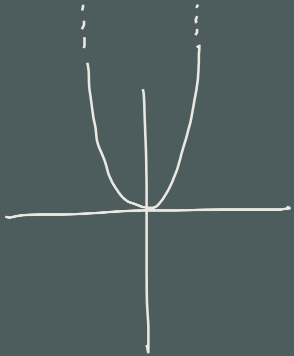
It's not as snappy, but these <u>projective schemes</u> add in the points we're missing.

It's not as snappy, but these <u>projective schemes</u> add in the points we're missing.

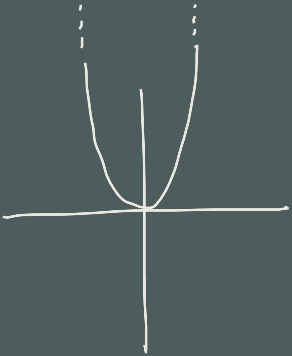
↳ let's see how with a simple example:

eg $y - x^2$

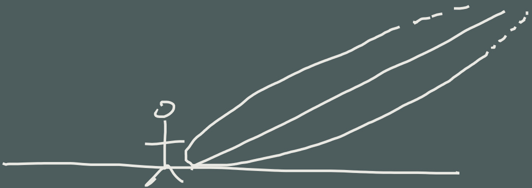
eg $y-x$



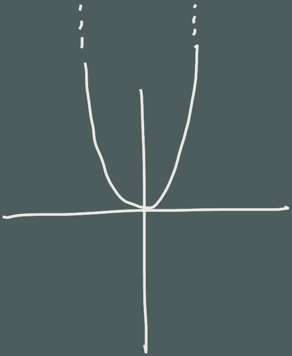
eg $y-x$



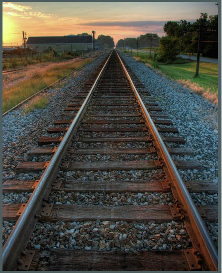
In perspective:



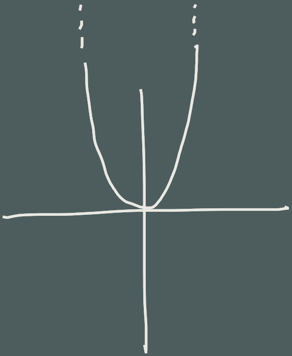
eg $y-x$



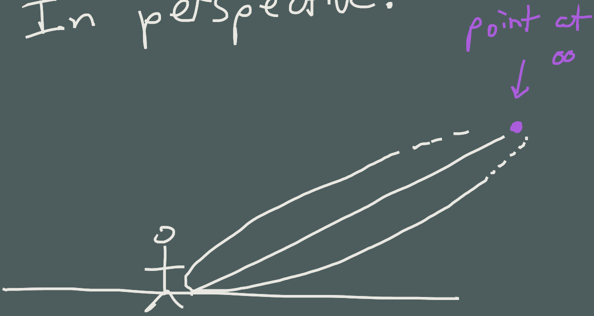
In perspective:

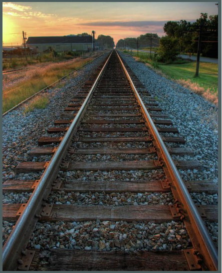


eg $y - x$



In perspective:





So

So let's count the points on

C = projective circle.

So let's count the points on

C = projective circle.

· homogenize:

So let's count the points on

C = projective circle.

- homogenize: $x^2+y^2-1 \rightsquigarrow x^2+y^2-z^2$

So let's count the points on

$\mathcal{C}$ = projective circle.

- homogenize: $x^2+y^2-1 \rightsquigarrow x^2+y^2-z^2$
- first we'll count points in the $z=1$ plane

<u>So</u> let's count the points on

C = <u>projective</u> circle.

- homogenize: $x^2+y^2-1 \rightsquigarrow x^2+y^2-z^2$
- first we'll count points in the $z=1$ plane
- then we'll count the "points at ∞" in the $z=0$ plane

<u>So</u> let's count the points on

C = <u>projective</u> circle.

- homogenize: $x^2+y^2-1 \rightsquigarrow x^2+y^2-z^2$
- first we'll count points in the $z=1$ plane
- then we'll count the "points at ∞" in the $z=0$ plane
- we'll assume $p \neq 2$.

<u>So</u> let's count the points on

C = <u>projective</u> circle.

- homogenize: $x^2+y^2-1 \rightsquigarrow x^2+y^2-z^2$
- first we'll count points in the $z=1$ plane
- then we'll count the "points at ∞" in the $z=0$ plane
- we'll assume $p \neq 2$.

(the $p=2$ case is actually <u>easier</u>, and a cute exercise)

when $z=1$:

when $z=1$:

$$x^2+y^2=1$$

when $z=1$:

$$x^2+y^2=1$$

$$y=\pm\sqrt{1-x^2}$$

when $z=1$:

$$x^2+y^2=1$$

$$y=\pm\sqrt{1-x^2}$$

$\Rightarrow$ want to know when $a=1-x^2$ has a square root in $\mathbb{F}_{p^n}$

when $z=1$:

$$x^2+y^2=1$$

$$y=\pm\sqrt{1-x^2}$$

$\Rightarrow$ want to know when $a=1-x^2$
has a square root in $\mathbb{F}_{p^n}$

$\Rightarrow$ thankfully, this is a
<u>very</u> well studied problem!

Define $\chi : \mathbb{F}_{p^n} \longrightarrow \{-1, 0, 1\}$

$$a \longmapsto \begin{cases} 0 & a = 0 \\ 1 & a = x^2 \ (\neq 0) \\ -1 & \text{otherwise} \end{cases}$$

Define $\chi : \mathbb{F}_{p^n} \to \{-1, 0, 1\}$

$$a \longmapsto \begin{cases} 0 & a = 0 \\ 1 & a = x^2 \ (\neq 0) \\ -1 & \text{otherwise} \end{cases}$$

$\hookrightarrow$ note $\chi(ab) = \chi(a) \cdot \chi(b)$

Define $\chi : \mathbb{F}_{p^n} \to \{-1, 0, 1\}$

$$a \longmapsto \begin{cases} 0 & a = 0 \\ 1 & a = x^2 \ (\neq 0) \\ -1 & \text{otherwise} \end{cases}$$

↳ note $\chi(ab) = \chi(a) \cdot \chi(b)$

↳ now we calculate:

$$\left|\{(x,y) \mid x^2+y^2=1\}\right| =$$

$$\left|\{(x,y) \mid x^2+y^2=1\}\right| = \sum_{a+b=1} \left|\{x^2=a\}\right| \cdot \left|\{y^2=b\}\right|$$

$$\left|\{(x,y) \mid x^2+y^2=1\}\right| = \sum_{a+b=1} \left|\{x^2=a\}\right| \cdot \left|\{y^2=b\}\right|$$

$$= \sum_{a+b=1} (1+\chi(a))(1+\chi(b))$$

$$\left|\{(x,y) \mid x^2+y^2=1\}\right| = \sum_{a+b=1} \left|\{x^2=a\}\right| \cdot \left|\{y^2=b\}\right|$$

$$= \sum_{a+b=1} (1+\chi(a))(1+\chi(b))$$

$$= \sum_{a+b=1} 1 + \chi(a) + \chi(b) + \chi(ab)$$

$$= \sum_{a} 1 + \chi(a) + \chi(1-a) + \chi(a(1-a))$$

$$\left|\{x^2+y^2=1\}\right| = \sum_a 1 + \chi(a) + \chi(1-a) + \chi(a(1-a))$$

$$= \sum_a 1 + \sum_a \chi(a) + \sum_a \chi(1-a) + \sum_a \chi(a(1-a))$$

$$\left|\{x^2+y^2=1\}\right| = \sum_a 1 + \chi(a) + \chi(1-a) + \chi(a(1-a))$$

$$= \sum_a 1 + \sum_a \chi(a) + \sum_a \chi(1-a) + \sum_a \chi(a(1-a))$$

$$= p^n + 0 + 0 + \sum_{a \neq 0,1} \chi(a(1-a))$$

$$
\left|\{x^2+y^2=1\}\right| = \sum_a 1 + \chi(a) + \chi(1-a) + \chi(a(1-a))
$$

$$
= \sum_a 1 + \sum_a \chi(a) + \sum_a \chi(1-a) + \sum_a \chi(a(1-a))
$$

$$
= p^n + \underbrace{0 + 0}_{\substack{\text{Summing a} \\ \text{character over} \\ \text{the whole group} \\ \text{gives } 0}} + \sum_{a \neq 0,1} \chi(a(1-a))
$$

$$|\{x^2+y^2=1\}| = \sum_a 1 + \chi(a) + \chi(1-a) + \chi(a(1-a))$$

$$= \sum_a 1 + \sum_a \chi(a) + \sum_a \chi(1-a) + \sum_a \chi(a(1-a))$$

$$= p^n + \underbrace{0 \quad + \quad 0}_{\substack{\text{Summing a}\\ \text{character over}\\ \text{the whole group}\\ \text{gives } 0}} + \underbrace{\sum_{a \neq 0,1} \chi(a(1-a))}_{\text{"error"}}$$

With some effort, we find

With some effort, we find

$$\text{error} = \sum_{a \neq 0,1} \chi(a(1-a)) = -\chi(-1).$$

With some effort, we find

$$\text{error} = \sum_{a \neq 0,1} \chi(a(1-a)) = -\chi(-1).$$

So #pts in the $z=1$ plane is

$$p^n - \chi(-1).$$

But a theorem of Euler says

$$\left(\text{in } \mathbb{F}_{p^n}\right)$$

$$\chi(-1) = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ (-1)^n & p \equiv 3 \bmod 4 \end{cases}$$

But a theorem of Euler says

$(\text{in } \mathbb{F}_{p^n})$

$$\chi(-1) = \begin{cases} 1 & p \equiv 1 \mod 4 \\ (-1)^n & p \equiv 3 \mod 4 \end{cases}$$

$$\text{So } \#\text{affine points} = \begin{cases} p^n + 1 & p \equiv 1 \bmod 4 \\ p^n - (-1)^n & p \equiv 3 \bmod 4 \end{cases}$$

So $\#\text{affine points} = \begin{cases} p^n + 1 & p \equiv 1 \bmod 4 \\ p^n - (-1)^n & p \equiv 3 \bmod 4 \end{cases}$

↳ you can check this agrees with our table!

	p^1	p^2	p^3	p^4	p^5
$p=2$	2	4	8	16	32
$p=3$	4	8	28	80	244
$p=5$	4	24	124	624	3124
$p=7$	8	48	344	2400	16808
$p=11$	12	120	1332	14640	161052

What about points at ∞?

What about points at ∞?

↳ Set $z=0$: $x^2+y^2=0$

What about points at ∞?

$\hookrightarrow$ Set $z=0$: $x^2+y^2=0$

in the $y=1$ plane:

What about points at ∞?

$\hookrightarrow$ set $z=0$: $x^2+y^2=0$

in the $y=1$ plane:

$x^2+1=0$

What about points at ∞?

↳ Set $z = 0$: $x^2 + y^2 = 0$

in the $y=1$ plane:

$x^2 + 1 = 0$,

so $x^2 = -1$

but we know

$$\exists x.\ x^2 = -1 \iff \chi(-1) = 1$$

$$\iff \begin{cases} p \equiv 1 \mod 4 \\ p \equiv 3 \mod 4,\ n \text{ even.} \end{cases}$$

So alltogether we get

$$|C(\mathbb{F}_{p^n})| = \#\text{affine pts} + \#\text{pts} @ \infty$$

$$= \begin{cases} (p^n - 1) + (2) & p \equiv 1 \bmod 4 \\ (p^n - (-1)^n) + (2 \cdot \mathbb{1}_{n \text{ even}}) & p \equiv 3 \bmod 4 \end{cases}$$

$$= p^n + 1$$

So alltogether we get

$$|C(\mathbb{F}_{p^n})| = \#\text{affine pts} + \#\text{pts @ } \infty$$

$$= \begin{cases} (p^n - 1) + (2) & p \equiv 1 \bmod 4 \\ (p^n - (-1)^n) + (2 \cdot \mathbb{1}_{n \text{ even}}) & p \equiv 3 \bmod 4 \end{cases}$$

$$= p^n + 1$$

(note the simplifying effect of the points at ∞)

Now, a classical idea:

Now, a classical idea:

When faced with a sequence of related numbers, look at the generating function!

Now, a classical idea:

When faced with a sequence of related numbers, look at the *generating function*!

(NB: The following is *not* the first generating function you might try... I have yet to see good "a priori" motivation for it, and would *Love* it if someone knows of some.)

$\underline{\text{Def}^{\underline{n}}}$:- (Hasse-Weil Zeta Function)

Def$^{\underline{n}}$:- (Hasse-Weil Zeta Function)

$$Z(X,t) \triangleq \exp\left(\sum_{n} |X(\mathbb{F}_{p^n})| \cdot \frac{t^n}{n}\right)$$

For us, then:

$$Z(\mathcal{C},t) = \exp\left(\sum_n |\mathcal{C}(\mathbb{F}_{p^n})| \cdot \frac{t^n}{n}\right)$$

For us, then:

$$Z(\mathcal{C},t) = \exp\left(\sum_n |\mathcal{C}(\mathbb{F}_{p^n})| \cdot \frac{t^n}{n}\right)$$

$$= \exp\left(\sum_n (p^n+1)\frac{t^n}{n}\right)$$

For us, then:

$$Z(C,t) = \exp\left(\sum_n |C(\mathbb{F}_{p^n})| \cdot \frac{t^n}{n}\right)$$

$$= \exp\left(\sum_n (p^n+1)\frac{t^n}{n}\right)$$

$$= \exp\left(-\log(1-pt) - \log(1-t)\right)$$

For us, then:

$$Z(\mathcal{C}, t) = \exp\left(\sum_n |\mathcal{C}(\mathbb{F}_{p^n})| \cdot \frac{t^n}{n}\right)$$

$$= \exp\left(\sum_n (p^n + 1)\frac{t^n}{n}\right)$$

$$= \exp\left(-\log(1-pt) - \log(1-t)\right)$$

$$= \frac{1}{(1-t)(1-pt)}$$

Now, some observations: $Z(C,t) = \dfrac{1}{(1-t)(1-pt)}$

Now, some observations: $Z(C,t) = \dfrac{1}{(1-t)(1-pt)}$

$\boxed{\text{I}}$ Z is <u>rational</u>!

Now, some observations: $Z(C,t) = \dfrac{1}{(1-t)(1-pt)}$

$\boxed{\text{I}}$ Z is <u>rational</u>!

write $Z = \dfrac{P_1}{P_0 \, P_2}$ with $P_0 = 1-t$
$P_1 = 1$
$P_2 = 1-pt$

Now, Some observations: $Z(\mathcal{C}, t) = \frac{1}{(1-t)(1-pt)}$

$\boxed{\mathrm{I}}$ Z is rational!

write $Z = \frac{P_1}{P_0 \, P_2}$ with $P_0 = 1-t$
$P_1 = 1$
$P_2 = 1-pt$

(note $2 = 2 \cdot \dim(\mathcal{C})$).

Now, some observations: $Z(C,t) = \frac{1}{(1-t)(1-pt)}$

$\boxed{\text{II}}$ each $P_k \in \mathbb{Z}[t]$ factors

as $\prod_j (1-\alpha_{jk} t)$ over $\mathbb{C}$

Now, some observations: $Z(C,t) = \frac{1}{(1-t)(1-pt)}$

$\boxed{\text{II}}$ each $P_k \in \mathbb{Z}[t]$ factors as $\prod_j (1-\alpha_{jk}t)$ over $\mathbb{C}$,

moreover, $|\alpha_{jk}| = p^{k/2}$ for each j.

Now, some observations: $Z(C,t) = \frac{1}{(1-t)(1-pt)}$

$$\boxed{\text{III}} \quad Z\left(\frac{1}{pt}\right) = pt^2 Z(t)$$

Now, some observations: $Z(C,t) = \frac{1}{(1-t)(1-pt)}$

$\boxed{III}$ $Z\left(\frac{1}{pt}\right) = pt^2 Z(t)$

moreover, the "2" here is the euler characteristic

$\chi(C(\mathbb{C})) = \chi(S^2) = 2.$

Now, some observations: $Z(C, t) = \dfrac{1}{(1-t)(1-pt)}$

$\boxed{\text{IV.}}$ Speaking of $C(\mathbb{C}) \cong S^2 \ldots$

Now, some observations: $Z(\mathcal{C}, t) = \frac{1}{(1-t)(1-pt)}$

$\boxed{\text{IV.}}$ Speaking of $\mathcal{C}(\mathbb{C}) \cong S^2 \ldots$

note

- $\deg \underline{P}_0 = 1 = \dim H^0(\mathcal{C}(\mathbb{C}))$
- $\deg \underline{P}_1 = 0 = \dim H^1(\mathcal{C}(\mathbb{C}))$
- $\deg \underline{P}_2 = 1 = \dim H^2(\mathcal{C}(\mathbb{C}))$.

§3

Really, what are the Weil Conjectures?

§3

Really, what are the Weil Conjectures?

Let X be a
- smooth
- projective
- n-dimensional

variety (over $\overline{\mathbb{F}_p}$).

Let X be a

- smooth
- projective
- n-dimensional

variety (over $\overline{\mathbb{F}}_p$).

the jacobian $\left[\frac{\partial f_\alpha}{\partial x_n}\right]$ has full rank

at each point of $X(\overline{\mathbb{F}}_p)$

Let X be a
- smooth
- projective
- n-dimensional

variety (over $\overline{\mathbb{F}}_p$).

Weil made the following conjectures (now theorems) about $Z(X,t)$.

$\boxed{\mathrm{I}}$ $Z(X,t)$ is rational, with

$$Z = \frac{P_1\, P_3 \cdots\ P_{2n-1}}{P_0\, P_2 \cdots P_{2n-2}\, P_{2n}}$$

where each $P_k \in \mathbb{Z}[t]$, and moreover

$P_0 = 1 - t$, $\quad P_{2n} = 1 - p^n t$

$\boxed{\text{II}}$ (Riemann Hypothesis)

each P_k factors as

$\prod_j (1-\alpha_{jk}t)$ over $\mathbb{C}$

and $|\alpha_{jk}| = p^{k/2}$ for each j.

$\boxed{\text{III.}}$ (functional equation)

$$Z\left(\frac{1}{p^n t}\right) = \pm p^{\frac{n\chi}{2}} t^{\chi} Z(t)$$

where

χ is the euler characteristic of $X(\mathbb{C})$

$\boxed{\mathrm{IV}}$ Lastly,

$$\deg(P_k) = \dim H^k(X(\mathbb{C}), \mathbb{Q})$$

where $H^\bullet$ is the cohomology of $X(\mathbb{C})$ with coefficients in $\mathbb{Q}$.

Notice the <u>constant</u> interplay

between

Notice the <u>constant</u> interplay between

- algebraic properties of $Z(X, t)$

Notice the <u>constant</u> interplay between

- algebraic properties of $Z(X, t)$

- geometric properties of $X(\mathbb{C})$

Notice the <u>constant</u> interplay between

- algebraic properties of $Z(X,t)$ $\leftarrow$ generating fn counting mod p^n solutions to polynomials

- geometric properties of $X(\mathbb{C})$

Notice the <u>constant</u> interplay between

- algebraic properties of $Z(X, t)$ ← generating fn counting mod p^n solutions to polynomials
- geometric properties of $X(\mathbb{C})$ ← a complex manifold.

How to use this?

How to use this?

Q How many solutions to

$$x_1x_6 - x_2x_5 + x_3x_4$$

in $\mathbb{F}_{p^n}$?

A

We recognize $X(G)$ as the plücker embedding of $Gr(2,4)$ inside $\mathbb{P}^5\mathbb{C}$.

$\underline{A}$

we recognize $X(\mathbb{C})$ as the plücker embedding of $Gr(2,4)$ inside $\mathbb{P}^5\mathbb{C}$.

$\hookrightarrow$ it doesn't matter if you know what this means! what matters is the <u>geometry</u> of $X(\mathbb{C})$ is well known!

- $\dim(X) = 8$

- $\dim(X) = 8$
- $\dim(H^n) = \begin{cases} 0 & n \text{ odd} \\ 2 & n = 4 \\ 1 & \text{otherwise} \end{cases}$

- $\dim(X) = 8$

- $\dim(H^n) = \begin{cases} 0 & n \text{ odd} \\ 2 & n = 4 \\ 1 & \text{otherwise} \end{cases}$

- $\chi = 6$

- $\dim(X) = 4$
- $\dim(H^n) = \begin{cases} 0 & n \text{ odd} \\ 2 & n = 4 \\ 1 & \text{otherwise} \end{cases}$
- $\chi = 6$

all of this is on the wikipedia page for "Grassmannian".

Then

$$Z(t) = \frac{1}{P_0 \, P_2 \, P_4 \, P_6 \, P_8}$$

Then

$$Z(t) = \frac{1}{P_0 P_2 P_4 P_6 P_8}$$

where $P_0 = 1 - t$, $P_8 = 1 - p^4 t$,

$\deg P_2 = \deg P_6 = 1$, and $\deg P_4 = 2$.

Then

$$Z(t) = \frac{1}{P_0 \, P_2 \, P_4 \, P_6 \, P_8}$$

where $P_0 = 1 - t$, $P_8 = 1 - p^4 t$,

$\deg P_2 = \deg P_6 = 1$, and $\deg P_4 = 2$.

write these as

$$P_2 = 1 - \alpha_2 t \quad P_4 = (1 - \alpha_{41} t)(1 - \alpha_{42} t) \quad P_6 = 1 - \alpha_6 t$$

If we hit both sides with log and taylor expand, we see:

$$\sum_n |X(\mathbb{F}_{p^n})| \frac{t^n}{n} = \sum_n (1+\alpha_2^n + \alpha_{41}^n + \alpha_{42}^n + \alpha_6^n + p^{4n}) \frac{t^n}{n}$$

If we hit both sides with log and taylor expand, we see:

$$\sum_n |X(\mathbb{F}_{p^n})| \frac{t^n}{n} = \sum_n (1+\alpha_2^n+\alpha_{41}^n+\alpha_{42}^n+\alpha_6^n+p^{4n})\frac{t^n}{n}$$

where, by the Riemann Hypothesis, $|\alpha_k| = p^{k/2}$

If we hit both sides with log and taylor expand, we see:

$$\sum_n |X(\mathbb{F}_{p^n})| \frac{t^n}{n} = \sum_n \left(1+\alpha_2^n+\alpha_{41}^n+\alpha_{42}^n+\alpha_6^n+p^{4n}\right)\frac{t^n}{n}$$

where, by the Riemann Hypothesis, $|\alpha_k| = p^{k/2}$

So $|X(\mathbb{F}_p^n)| = p^{4n} \pm O(p^{3n})$

If we hit both sides with log and taylor expand, we see:

$$\sum_n |X(\mathbb{F}_{p^n})| \frac{t^n}{n} = \sum_n (1+\alpha_2^n + \alpha_{41}^n + \alpha_{42}^n + \alpha_6^n + p^{4n}) \frac{t^n}{n}$$

where, by the Riemann Hypothesis, $|\alpha_k| = p^{k/2}$

So $|X(\mathbb{F}_p^n)| = p^{4n} \pm O(p^{3n})$

(and if we calculated the α_k, which is effective, we would know the <u>exact</u> answer!)

So how do we prove this!?

So how do we prove this!?

"A"

recall $\mathbb{F}_{p^n} = \{ x \in \overline{\mathbb{F}_p} \mid \phi^n x = x \}$,

for the Frobenius map $\phi(x) = x^p$.

So how do we prove this!?

"A"

recall $\mathbb{F}_{p^n} = \{ x \in \overline{\mathbb{F}_p} \mid \phi^n x = x \}$,

for the Frobenius map $\phi(x) = x^p$.

So we want to count the fixed points

of $\phi^n : X(\overline{\mathbb{F}_p}) \to X(\overline{\mathbb{F}_p})$.

So how do we <u>prove</u> this!?

"<u>A</u>" recall $\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}}_p \mid \phi^n x = x\}$,

for the <u>Frobenius map</u> $\phi(x) = x^p$.

So we want to count the fixed points of $\phi^n : X(\overline{\mathbb{F}}_p) \to X(\overline{\mathbb{F}}_p)$.

$\hookrightarrow$ Lefshetz!

$$\left|\{x \in X \mid fx = x\}\right| = \sum_{k=0}^{2n} (-1)^k \operatorname{tr}\left(f^* \mid H^k\right)$$

$$\left|\{x \in X \mid fx = x\}\right| = \sum_{k=0}^{2n} (-1)^k \operatorname{tr}\left(f^* \mid H^k\right)$$

So for us,

$$\left|X(\mathbb{F}_{p^n})\right| = \sum_{k=0}^{2n} (-1)^k \operatorname{tr}\left(\phi^{n*} \mid H^k\right)$$

$$|\{x \in X \mid fx = x\}| = \sum_{k=0}^{2n} (-1)^k \operatorname{tr}(f^* \mid H^k)$$

So for us,

$$|X(\mathbb{F}_{p^n})| = \sum_{k=0}^{2n} (-1)^k \operatorname{tr}(\phi^{n*} \mid H^k)$$

When we hit this with exp,

$\Sigma \rightsquigarrow \Pi$, and $\operatorname{tr} \rightsquigarrow \det$.

$$Z(X,t) = \frac{\prod_{k \text{ odd}} \det\left(1-\phi^* t \mid H^k\right)}{\prod_{k \text{ even}} \det\left(1-\phi^* t \mid H^k\right)}$$

$$Z(X,t) = \frac{\prod_{k \text{ odd}} \det(1-\phi^* t \mid H^k)}{\prod_{k \text{ even}} \det(1-\phi^* t \mid H^k)}$$

So define $P_k = \det(1-\phi^* t \mid H^k)$

and we have $\boxed{\mathrm{I}}$!

$\boxed{\text{III}}$ is basically Poincaré Duality

$\boxed{III}$ is basically poincaré Duality

$\boxed{IV}$ is because the degree of a characteristic polynomial is the dimension of your vector space

$\boxed{III}$ is basically Poincaré Duality

$\boxed{IV}$ is because the degree of a characteristic polynomial is the dimension of your vector space

$\boxed{II}$ is trickier - follows from a theorem of Serre.

↳ Of course, this proof can't work.

↳ Of course, this proof can't work.

↳ $X(\overline{\mathbb{F}}_p)$ isn't actually a manifold.

↳ Of course, this proof can't work.

↳ $X(\overline{\mathbb{F}}_p)$ isn't <u>actually</u> a manifold.

↳ so there's no cohomology theory for it

↳ Of course, this proof can't work.

↳ $X(\overline{\mathbb{F}}_p)$ isn't actually a manifold.

↳ so there's no cohomology theory for it

↳ ... unless ...

§4

In which we show there <u>is</u> a cohomology theory for it!

In his Tōhoku paper, Grothendieck found an axiomatic framework for cohomology theories.

↳ defined abelian categories

↳ defined <u>abelian categories</u>

↳ Showed how to get a cohomology theory for any (left-exact, additive) functor $\mathfrak{A} \to \mathfrak{B}$

↳ defined abelian categories

↳ Showed how to get a cohomology theory for any (left-exact, additive) functor $\mathfrak{A} \to \mathfrak{B}$

↳ provided $\mathfrak{A}$ has "enough injectives"

↳ showed any $\mathfrak{A}$ satisfying his axiom AB5 (with a generator) has enough injectives.

↳ Showed any $\mathfrak{A}$ satisfying his axiom AB5 (with a generator) has enough injectives.

↳ <u>Also</u> showed for any space X, the category of sheaves of abelian groups on X satisfies AB5

↳ Showed any $\mathfrak{A}$ satisfying
his axiom AB5 (with a generator)
has enough injectives.

↳ Also showed for any space X,
the category of sheaves of
abelian groups on X satisfies AB5

↳ the cohomology of $\Gamma(X,-)$ is classical
sheaf cohomology!

↳ Serre finds a way to build an H^1, using "unramified covers".

↳ Serre finds a way to build an H^1, using "unramified covers".

↳ Grothendieck knows that covers $\approx$ sheaves.

But where there's sheaves, there's an AB5 category, and there's cohomology!

The idea, then?

The idea, then?

↳ Redo the idea of sheaves in a more general setting.

The idea, then?

↳ Redo the idea of sheaves in a more general setting.

↳ then redo the proof that sheaves of abelian groups are AB5

The idea, then?

↳ Redo the idea of Sheaves in a more general setting.

↳ then redo the proof that sheaves of abelian groups are AB5

↳ ???

The idea, then?

↳ Redo the idea of Sheaves in a more general setting.

↳ then redo the proof that sheaves of abelian groups are AB5

↳ ???

↳ get cohomology: profit.

Recall, a sheaf on (X, τ) is a map $F : \tau \longrightarrow \text{Set}$ so that

- if $U \subseteq V$, then $FV \subseteq FU$
- if $\{U_\alpha\}$ is an open cover of U, and if the $f_\alpha \in FU_\alpha$ are compatible in the sense that $f_\alpha \restriction U_\alpha \cap U_\beta = f_\beta \restriction U_\alpha \cap U_\beta$ then $\exists! \, f \in FU$ so that $f_\alpha = f \restriction U_\alpha$

eg $\mathbb{F}U \triangleq \{ f : U \to \mathbb{R} \text{ cts} \}.$

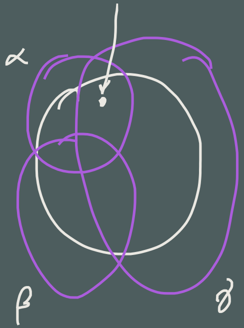
eg $\mathbb{F}U \triangleq \{f : U \to \mathbb{R} \text{ cts}\}$.

$\hookrightarrow$ if the $\{U_\alpha\}$ cover U,
f_α is defined on each U_α,
and the f_αs agree on
intersections, then we can
glue them together into a
map on U.

eg $\mathbb{F}U \triangleq \{f : U \to \mathbb{R} \text{ cts}\}$.

↳ if the $\{U_\alpha\}$ cover U, f_α is defined on each U_α, and the f_αs agree on intersections, then we can glue them together into a map on U.

need $f_\alpha x = f_\beta x$



So to define sheaves, we really need

So to define sheaves, we really need

- "open sets"

So to define sheaves, we really need

- "open sets"
- When do $\{U_\alpha\}$ "cover" U?

So to define sheaves, we really need

- "open sets"
- When do $\{U_\alpha\}$ "cover" U?
- When do U_α, U_β "overlap"?

<u>Def$^{\underline{n}}$</u>

if $\mathcal{C}$ is a (small) category,

a <u>Grothendieck Topology</u> on $\mathcal{C}$

is a choice $j(U)$ of subfunctors

of $\mathcal{C}(-, U)$, called "covering families",

satisfying natural coherence conditions

Then, immitating the Classical def^{n},
we define a <u>sheaf</u> on $(\mathcal{C}, j)$
to be a functor $\mathbb{F} : \mathcal{C}^{op} \to Set$
So that whenever $R \in j(U)$,

$$\begin{tikzcd} R \arrow[r, tail] \arrow[dr, "\alpha"'] & \mathcal{C}(-,U) \arrow[d, dashed, "\bar{\alpha}"] \\ & \mathbb{F} \end{tikzcd}$$

every $\alpha : R \to \mathbb{F}$ extends to $\mathcal{C}(-,U)$

↳ recall, by yoneda,

$$\{\bar{\alpha} : \mathrm{Hom}(-,U) \to F\} \longleftrightarrow \{FU\}$$

and $R \rightarrowtail \mathrm{Hom}(-,U)$ is "really"
a family of objects mapping to U
(think of when $\mathcal{C}$ is a poset)

Now we can define $\underline{Sh(\mathcal{C}, j)}$

to be the category of sheaves on $(\mathcal{C}, j)$

Now we can define $\underline{Sh(\mathcal{C}, j)}$ to be the category of sheaves on $(\mathcal{C}, j)$

A category $\mathcal{E}$ equivalent to some $Sh(\mathcal{C}, j)$ is called a <u>Grothendieck Topos</u>

Then we can define the category of abelian groups in $\mathcal{E}$, $ab(\mathcal{E})$

Then we can define the category of abelian groups in $\mathcal{E}$, $ab(\mathcal{E})$

$\hookrightarrow$ the same argument from Tōhoku shows $ab(\mathcal{E})$ satisfies AB5

Then we can define the category of abelian groups in $\mathcal{E}$, $ab(\mathcal{E})$

↳ the same argument from Tōhoku shows $ab(\mathcal{E})$ satisfies AB5

↳ Then the "global sections functor" $Hom(1,-)$ becomes a left-exact additive functor

$$ab(\mathcal{E}) \longrightarrow ab(Set)$$

$\hookrightarrow$ So it has a cohomology theory!

↳ So it has a cohomology theory!

↳ in fact, it's exactly this cohomology that gets the job done.

↳ So it has a cohomology theory!

↳ in fact, it's exactly this cohomology that gets the job done.

↳ let's see just a <u>little</u> more!

Write $\acute{E}t/_X$ for the category whose objects are étale maps $U \to X$ and whose arrows are maps $U_1 \to U_2$ so that

$$\begin{tikzcd} U_1 \arrow[rr] \arrow[dr] & & U_2 \arrow[dl] \\ & X & \end{tikzcd}$$

Commutes.

Now we say a family

$\{\varphi_\alpha : U_\alpha \to U\}$ <u>covers</u> U iff

$$\bigcup_\alpha \varphi_\alpha[U_\alpha] = U$$

Now we say a family

$\{\varphi_\alpha : U_\alpha \to U\}$ covers U iff

$$\bigcup_\alpha \varphi_\alpha[U_\alpha] = U$$

↳ this is a Grothendieck topology on $\acute{E}t/X$.

The resulting cohomology theory is enough like classical cohomology for the "proofs" of $\boxed{\text{I}}$, $\boxed{\text{III}}$, and $\boxed{\text{IV}}$ to go through!

But.

Not the Riemann Hypothesis $\boxed{\text{II}}$.

But:

Not the Riemann Hypothesis $\boxed{\text{II}}$.

↳ this was proved separately by Deligne, though these ideas are present in his proof.

There is a set of "Standard Conjectures" which, if true, will let us prove $\boxed{\text{II}}$ formally!

There is a set of "Standard Conjectures" which, if true, will let us prove $\boxed{\text{II.}}$ formally!

↳ unfortunately, almost all of them are <u>wide</u> open!

Thank You