Topos Theory and the Weil Conjectures

Chris Grossack
(they/them)

December 3, 2021

1 What Are The Weil Conjectures?

One of the oldest problems in number theory is that of solving diophantine equations. That is, given a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, when does it have integer solutions? If f does have integer solutions, natural follow up questions include "how many solutions?", and "what are they?". If instead f does *not* have integer solutions, a natural follow up is "why not?", and one of the oldest answers to this question is a "mod n obstruction". If f has a solution in $\mathbb{Z}$, then by reducing everything in sight mod n, we would also get a solution mod n for every n. Thus, if we can show that f has no solution mod n (which requires only a finite check!), it cannot have a solution in $\mathbb{Z}$[1].

Since the chinese remainder theorem allows us to decompose $\mathbb{Z}/n$ into products of $\mathbb{Z}/p^k$, where p is a prime, we restrict attention to those. Of course, by Hensel's lemma it is often enough to restrict attention to just $\mathbb{Z}/p$, which has extra nice properties since it is a field. Thus we are naturally led to the problem of solving polynomials over the prime fields $\mathbb{F}_p = \mathbb{Z}/p$. The fields $\mathbb{F}_q = \mathbb{F}_{p^k}$, are created by adding roots of polynomials to $\mathbb{F}_p$, and it is then reasonable to ask how the number of solutions to f changes as we move between the $\mathbb{F}_q$ for $q = p, p^2, p^3, p^4, \dots$.

As an example, let's consider the polynomial $f = x^2 + y^2 - 1$. We can ask a computer algebra system like Sage to check how many solutions there are over various finite fields:

	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

[1] After hearing this, it's natural to ask if this is the *only* obstruction. That is, if f has a solution mod n for every n, must it have a solution in $\mathbb{Z}$? It turns out the answer is "no", but a discussion of this phenomenon would take us beyond the scope of this article.

If we write N_q to mean the number of solutions in $\mathbb{F}_q$, then notice $N_q \approx q$, with an error of at most ± 1! Writing this as $N_q = q + \text{error}$, the Weil Conjectures give us tight control over this error term. But (perhaps surprisingly) this error term depends on the *geometry* of the complex solutions to the polynomial f viewed as a complex manifold!

In fact, everything we're about to do will also be true for the simultaneous solution set of a *family* of polynomials (called a variety). Still, for conceptual clarity, we will work with an affine curve for all of our examples.

1.1 A Concrete Computation

Following an argument in [21], we can compute N_{p^k} for p an odd prime. Our job is to count the points $\{(x, y) \in \mathbb{F}_{p^k}^2 \mid x^2 + y^2 - 1 = 0\}$. Said another way, we're trying to solve the equation $y^2 = 1 - x^2$, and there are 3 cases to consider:

- $1 - x^2 = 0$
- $1 - x^2 \neq 0$ is a square
- $1 - x^2$ is not a square

In the first case, $y = 0$ is the only solution, in the second, both of $y = \pm\sqrt{1 - x^2}$ work, and of course there are no solutions in the third case.

Inspired by this trichotomy, we consider the character $\chi : \mathbb{F}_{p^k} \to \{-1, 0, 1\}$ defined by

$$\chi(a) = \begin{cases} 0 & a = 0 \\ 1 & a \neq 0 \text{ is a square in } \mathbb{F}_{p^k} \\ -1 & \text{otherwise} \end{cases}$$

Now, conveniently, we see that $|\{y \in \mathbb{F}_{p^k} \mid y^2 = a\}| = 1 + \chi(a)$, and so we find

$$\begin{aligned} |N_{p^k}| &= |\{(x, y) \mid x^2 + y^2 = 1\}| \\ &= \sum_{a_1 + a_2 = 1} |\{x^2 = a_1\}||\{y^2 = a_2\}| \\ &= \sum_{a_1 + a_2 = 1} (1 + \chi(a_1))(1 + \chi(a_2)) \\ &= p^k + \sum_{a_1 \neq 0, 1} \chi(a_1)\chi(1 - a_1) \end{aligned}$$

where in the last sum we've expanded the product and used the fact that χ is a character to show two of the resulting sums are 0. See [21] for a more detailed explanation of this calculation.

Notice this agrees with our earlier table of values, where we found $|N_{p^k}| \approx p^k$. In fact, the cited article goes on to show that

$$|N_{p^k}| = p^k - \chi(-1)$$

which we can simplify further, since we know exaclty when -1 is a square.

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

which finally tells us

$$|N_{p^k}| = \begin{cases} p^k - 1 & p \equiv 1 \pmod 4 \\ p^k - (-1)^k & p \equiv 3 \pmod 4 \end{cases}$$

which perfectly matches our table.

1.2 A Geometric Interlude

When we're working over a more classical field, like $\mathbb{R}$ or $\mathbb{C}$, then a system of polynomial equations (in n variables) carves out a set in $\mathbb{R}^n$ or $\mathbb{C}^n$. For instance, the solutions to our example $x^2 + y^2 - 1$ carves out exactly the unit circle in $\mathbb{R}^2$. It turns out that sometimes an equation will have "points at infinity" that really belong on the curve, and make the geometric set of solutions much simpler[2]. We can add these points at infinity by consdering solutions in the Projective Space $\mathbb{P}^n_{\mathbb{C}}$, and by working with the homogenized versions of our polynomials.

The sets we get in this way turn out to be complex manifolds, with the exception of some singular points. We have access to more geometric tools when our varieties are nonsingular everywhere, and this happens exactly when the derivative of f never vanishes on the solution set. In the case of a variety carved out by multiple polynomials $f_1, \ldots, f_n$, this happens exactly when the *jacobian* never vanishes on the solution set. As usual, we call a variety without singular points smooth.

At this point, it is useful to introduce slightly more notation in order to make things clear going forwards. If X is a variety defined by integer polynomials and k is some field[3] we write $X(k)$ to mean the set of k-solutions to the polynomials defining X. Then we're interested in understanding how $|X(\mathbb{F}_{p^k})|$ changes as we vary k.

For a simple example, let's say that f is a polynomial in $n+2$ variables $x_0, \ldots x_{n+1}$. That means the hypersurface $X(\mathbb{C})$ defined by f will be an n-dimensional variety in $\mathbb{P}^{n+1}_{\mathbb{C}}$, which we'll moreover assume is smooth. Intuitively, we expect an n-dimensional variety to look roughly like $\mathbb{A}^n_{\mathbb{C}}$ (affine n-space), which is a fancy name for $\mathbb{C}^n$.

Interestingly, in the computation for N_q for f, we found

[2]Though, again, we don't have space in this article to detail why

[3]More generally some ring, but we won't have need for that generality here

$$N_q \approx q = |\mathbb{A}_{\mathbb{F}_q}| = |\mathbb{F}_q|.$$

Indeed, if we were to work out some more examples, we would see that for an n dimensional variety, we always have

$$N_q \approx q^n = |\mathbb{A}^n_{\mathbb{F}_q}| = |\mathbb{F}_q|^n.$$

This might lead us to conjecture that, for a smooth variety X, the number of $\mathbb{F}_q$ points of X should be roughly $q^{\dim(X)}$. That is,

$$|X(\mathbb{F}_{p^k})| \approx p^{k \dim(X)}.$$

Let's return to the special case of the circle $x^2 + y^2 - 1$ and try to formalize the relationship between the numbers $|X(\mathbb{F}_{p^k})|$. Slightly more generally, we can ask about (nonsingular, connected) algebraic curves. It seems ambitious to ask for a nice formula, but in many concrete examples we get the next best thing: a nice *generating function*[4].

Definition 1. Define the (Hasse-Weil) Zeta Function by

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

//

1.3 A Concrete Computation (Continued)

Recall from the last concrete computation that for odd primes, (using our new notation),

$$|X(\mathbb{F}_{p^k})| = \begin{cases} p^k - 1 & p \equiv 1 \pmod 4 \\ p^k - (-1)^k & p \equiv 3 \pmod 4 \end{cases}$$

where X is the circle, defined by $x^2 + y^2 - 1$.

Then we can compute for $p \equiv 1 \pmod 4$:

$$\begin{aligned} Z(X,t) &= \exp\left(\sum_k (p^k - 1)\frac{t^k}{k}\right) \\ &= \exp\left(\log(1-t) - \log(1-pt)\right) \\ &= \frac{1-t}{1-pt} \end{aligned}$$

[4]We considered including more tables with explicit computations in this note, but it seemed unnecessary given the excellent surveys [16] and [21]

and for $p \equiv 3 \pmod 4$:

$$\begin{aligned} Z(X,t) &= \exp\left(\sum_k (p^k - (-1)^k)\frac{t^k}{k}\right) \\ &= \exp\left(\log(1+t) - \log(1-pt)\right) \\ &= \frac{1+t}{1-pt} \end{aligned}$$

2 No Really, *What Are The Weil Conjectures?*

In the above example we computed $Z(X,t)$ in the case of the (affine) circle $X = \{x^2+y^2 = 1\}$. Already we can see lots of structure, such as the rationality of Z, but things become even nicer when we pass to projective curves X, and thus allow certain "points at infinity" to count towards our total.

How nice do things become? Well, it's time to formally state the Weil Conjectures[5]:

Let X be a smooth, connected, n-dimensional projective variety over $\mathbb{F}_p$. Then

1. (Rationality) $Z(X,t)$ is a rational function given by $Z(X,t) = \frac{P_1 P_3 P_5 \cdots P_{2n-1}}{P_0 P_2 \cdots P_{2n}}$ with each $P_k \in \mathbb{Z}[t]$. Moreover, $P_0 = 1 - t$ and $p_{2n} = 1 - p^n t$
2. (Riemann Hypothesis) Over $\mathbb{C}$, each P_k factors as $\prod_j (1 - \alpha_{kj} t)$ with $|\alpha_{kj}| = p^{\frac{k}{2}}$
3. (Functional Equation) $Z\left(X, \frac{1}{p^n t}\right) = \pm p^{\frac{n\chi}{2}} t^\chi Z(X,t)$, where χ is the Euler characteristic of X
4. (Betti Numbers) If in addition, the polynomials defining X are the mod-p reduction of polynomials defining a smooth complex manifold $X(\mathbb{C})$, then we have $\deg(P_i) = \dim_{\mathbb{Q}} H^i(X(\mathbb{C}), \mathbb{Q})$, where $\dim_{\mathbb{Q}} H^i(X(\mathbb{C}), \mathbb{Q})$ is the ith Betti number of $X(\mathbb{C})$.

2.1 A Quick Aside: What Does This Have To Do With The Riemann Hypothesis?

If we think of $\mathbb{Z}$ as the ring of functions on the curve spec$\mathbb{Z}$, then the classical Riemann Zeta Function becomes

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

[5] which have all been proven, despite the historical name

which we rewrite in terms of the closed points of spec$\mathbb{Z}$

$$\zeta(s) = \prod_{\mathfrak{p} \in \text{spec}\mathbb{Z} \text{ closed}} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

where $N(\mathfrak{p}) = p = |\mathbb{Z}/\mathfrak{p}|$.

Now, let's say X is an (affine[6]) curve over $\mathbb{F}_p$. Then by analogy, we should consider the function

$$\zeta_X(s) \triangleq \prod_{\mathfrak{p} \in \mathbb{F}_p[X]} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

where now $\mathbb{F}_p[X]$ is the coordinate ring of X, and we use a slightly more general notion of $N(\mathfrak{p})$, since the possible quotients of $\mathbb{F}_p[X]$ are more complicated than the possible quotients of $\mathbb{Z}$. In particular, we say $N(\mathfrak{p}) = p^r = |\mathbb{F}_{p^r}|$ whenever r is minimal with $\mathbb{F}_p[X]/\mathfrak{p} \subseteq \mathbb{F}_{p^r}$.

Then the punchline is this:

$$\zeta_X(s) = Z(X, p^{-s}).$$

Now, the zeroes of $\zeta_X(s) = Z(S, p^{-s})$ occur when the numerator is 0, and this happens when one of the $P_k(p^{-s}) = 0$ for k odd. But now the "Riemann Hypotehsis" part of the Weil conjectures tells us when this happens!

Each P_k factors as $\prod_j (1 - \alpha_{kj} t)$ with $|\alpha_{kj}| = p^{\frac{k}{2}}$. So if $P_k(p^{-s}) = 0$, we must have $\alpha_{kj} p^{-s} = 1$, and taking norms we see

$$p^{\sigma} = p^{\frac{k}{2}}$$

where σ is the real part of s.

So then the "Riemann Hypothesis" tells us the zeroes of $\zeta_X(s)$ can only occur when the real part of s is $\frac{k}{2}$. This is clearly analogous to the classical Riemann Hypothesis, which claims that the nontrivial[7] zeroes of $\zeta(s)$ only occur when the real part of s is $\frac{1}{2}$.

Similarly, using this new notation, the Functional Equation says that

$$\zeta_X(s) = \pm p^{s\chi - \frac{n\chi}{2}} \zeta_X(n - s)$$

[6] spec$\mathbb{Z}$ is not compact in any reasonable sense, and it behaves like an affine curve rather than a projective one. To that end, we go back to considering affine curves for this part of the notes. Interestingly, some number theorists believe that the key to solving the Riemann Hypothesis lies in finding a suitable "compactification" of spec$\mathbb{Z}$. See, for instance, the excellent survey [3]

[7] The presence of the trivial zeroes is related again to the fact that spec$\mathbb{Z}$ is not compact. Just as we often consider $\pi^{-s/2}\Gamma(s/2)\zeta(s)$, which removes the nontrivial zeroes, when we pass from an affine curve to a projective curve, we multiply ζ_X by a new rational function which kills some zeroes.

which is, again, reminiscent of the classical functional equation

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s)$$

2.2 A Remarkable "Proof"

Even though these conjectures are fairly easy to state, as they only have to do with generating functions counting solutions to polynomial equations, they require remarkably powerful machinery to prove. Even in the case of curves, the original proof used high dimensional algebraic geometry before later being simplified to a proof that "only" uses Riemann-Roch. See [18] for a proof in the case of curves, [16] for a historical account, and the excellent lecture series [19] for another overview.

This said, there is a jaw-dropping informal argument for why these conjectures might be true[8]:

From Galois theory, recall the elements of $\mathbb{F}_{p^n}$ are exactly the fixed points of an algebraic closure $\overline{\mathbb{F}_p}$ under the map ϕ^n, where $\phi : x \mapsto x^p$ is the Frobenius Endomorphism.

Then if X is given by the solutions of some family of polynomials with coefficients in $\mathbb{F}_p$, it's easy to see ϕ maps $X(\overline{\mathbb{F}_p})$ to itself. So then the $\mathbb{F}_{p^n}$ points $X(\mathbb{F}_{p^n})$ will be given by exactly the fixed points of $X(\overline{\mathbb{F}_p})$ under ϕ^n.

Now, let's imagine that $\phi : X(\overline{\mathbb{F}_p}) \to X(\overline{\mathbb{F}_p})$ was actually a map of smooth $\mathbb{C}$-varieties. Then we know how to count the fixed points of ϕ^n! We can use the Lefschetz Fixed Point Formula:

$$|X(\mathbb{F}_{p^n})| = |\{x \in X(\overline{\mathbb{F}_p}) \mid \phi^n x = x\}| = \sum_{j=0}^{2n} (-1)^j \mathrm{Tr}\big((\phi^n)^*; H^j(X, \mathbb{Q})\big)$$

Now plugging this into the definition of $Z(X,t)$, and recalling that $\exp(\mathrm{Tr}(A)) = \det(A)$, we find

$$Z(X,t) = \frac{\prod_{j \text{ odd}} \det(1 - (\phi)^* t; H^j(X, \mathbb{Q}))}{\prod_{j \text{ even}} \det(1 - (\phi)^* t; H^j(X, \mathbb{Q}))}$$

If we define $P_j(t) = \det(1 - (\phi^n)^* t; H^j(X, \mathbb{Q}))$, then we recover part 1 of the Weil Conjectures!

Part 3 follows from Poincare Duality, and Part 2 follows from a theorem of Serre which says that, under certain conditions (formally satisfied by ϕ), the eigenvalues of ϕ^* on $H^j(X, \mathbb{Q})$ have absolute value $q^{\frac{j}{2}}$.

Of course, this proof is meaningless because the cohomology theories for $\mathbb{C}$ varieties are not applicable to varieties over finite fields. Weil himself thought that this proof was

[8] The reader who is familiar with Sophie Morel's excellent lecture [8] will doubtless recognize its influence on this section

suggestive, but un-formalizable, and was looking for other avenues of proof. Serre, Artin, and Grothendieck, however, believed that this analogy was too beautiful to be incorrect, and set out to create a cohomology theory that would work for more general varieties. If they succeeded, then this informal argument would be able to be pushed through in an entirely precise way.

After a lot of work, Étale Cohomology was born, and with it came the solution to parts 1, 3, and 4 of the Weil Conjectures. Interestingly, the theory is unable to prove the Riemann Hypothesis in its current form. There are a set of problems, humorously called the "standard conjectures" which would give an Étale Cohomological proof of the Riemann Hypothesis for varieties, but almost all of these have been open for the past 60 years. Instead, Deligne found a way to sidestep these conjectures, and prove the Riemann Hypothesis directly!

In the second half of this note, we'll spend some time talking about the machinery that was eventually used in order to prove the Weil conjectures: That of Topos Theory.

3 Abelian Categories and Cohomology

After seeing the "proof" from the last section, mathematicians embarked on a hunt for a cohomology theory that was formally similar to classical cohomology and that worked for varieties over finite fields!

There was a zoo of cohomology theories in the air at the time, all of which seemed to accomplish similar goals with fairly different initial data. Grothendieck's famous Tôhoku paper showed that many of these theories are all particular instances of a more abstract theory, which has since matured into homological algebra.

Of particular relevance to us is the notion of an AB5 category, a kind of abelian category[9] that always has enough injectives. This is useful because if $\mathcal{A}$ is an ablian category with enough injectives and $F : \mathcal{A} \to \mathcal{B}$ is a left exact additive functor, we can associate to F its Derived Functors R^iF as follows. Here A is an object in $\mathcal{A}$:

1. Fix an injective resolution $A \to I^0 \to I^1 \to \cdots$
2. Hit the chain complex $I^\bullet$ with F to get a chain complex $(FI^\bullet, d^\bullet)$ of objects in $\mathcal{B}$
3. Define R^iFA to be the cokernel of the unique mono $\operatorname{im} d^{i-1} \rightarrowtail \ker d^i$

As a motivating example, consider a topological space X. Then the category of sheaves of abelian groups on X forms an AB5 category, and thus has enough injectives. If we fix a sheaf $\mathcal{F}$ on X, then we can define the cohomology $H^i(X, \mathcal{F})$ as $R^i\Gamma$, where Γ is the functor taking a sheaf of abelian groups on X to the "global section", the abelian group associated to the open set X. This gives us "classical" sheaf cohomology, from which we can recover the (even more classical) cohomology of a topological space by considering constant sheaves.

[9] An abelian category is one that shares many nice properties with the category of abelian groups. For a more precise definition of this any many other aspects of cohomology we will be glossing over in this note, see [22].

Grothendieck knew that sheaf cohomology could be formulated in this way, and moreover had a good idea of what parts of the sheaf category were needed to prove that it was AB5. When Serre gave a talk explaining how to get one dimensional cohomology groups H^1 by using "unramified covers" of schemes, Grothendieck saw these generalized covering spaces as the key to the entire project. The idea was deceptively simple:

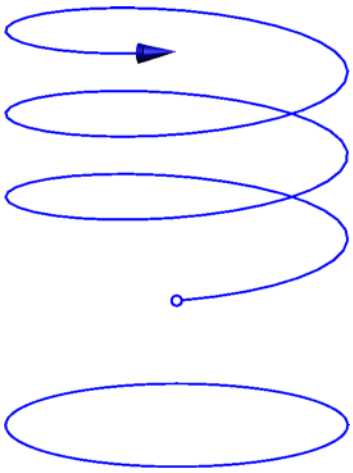
Sheaves and Étale spaces are the same thing (up to equivalence). Moreover, the category of sheaves of abelian groups on X is AB5, thus has a canonical cohomology theory. Now that Grothendieck has seen these unramified covers, he thinks to build a more general notion of "sheaf category" on a scheme X whose Étale spaces will be these coverings. Then, if all is right with the universe, the category of abelian groups of these more general sheaves will *still* be AB5! In which case they'll have a cohomology theory, which *must* be the right one.

At this point we depart somewhat from the historical development to give a modern view of these generalized sheaf categories, now called Grothendieck Toposes, but we point the historically inclined reader to the (excellent) talk [6] by Colin McLarty.

4 Toposes and Cohomology

A topos is many things to many people, which is part of the appeal of the subject. For us, we will focus exclusively on the features of the theory which are useful for defining Étale cohomology, though it pains my logician's heart. We start with sheaf categories on a topological space, as these will be the objects which we generalize.

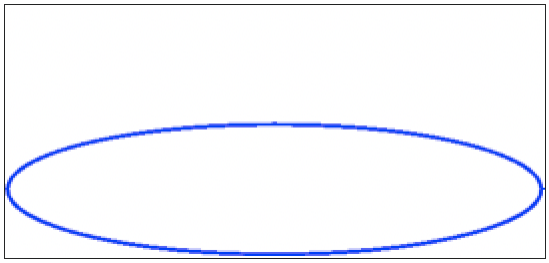
If X is a topological space, we write $\mathsf{Sh}(X)$ for the category of (Set-valued) sheaves on X. Again, we find these are equivalent to the Étale spaces on X. That is, topological spaces Y equipped with a map $Y \to X$ so that each point in Y has a neighborhood homeomorphic to its image in X. In the case $X = S^1$ is the unit circle, there are a number of useful examples, but here is one nice one:



Notice in particular that this is *not* a covering space! While it's true that every covering space is Étale, we can get by with something slightly weaker. For instance, here every point "upstairs" has a neighborhood homeomorphic to a neighborhood "downstairs" in S^1. However

every point in S^1 need *not* have a neighborhood whose preimage looks like a disjoint union of copies of itself. The point below the open endpoint of this half-helix, for instance, will not have that property.

As a more extreme example of the same phenomenon, consider the following Étale space:



Here the fibre over every point is *empty*. This is an initial object in $\mathsf{Sh}(X)$, but is not a covering space for the same reason as before. The terminal object in $\mathsf{Sh}(X)$ is given by the sheaf with one point in each fibre. This corresponds to the Étale space $X \to X$ by the identity, and so we can consider the terminal object in $\mathsf{Sh}(X)$ as a kind of analogue of X itself.

A more general way to phrase the notion of a sheaf is as a special kind of functor. This will be the foundation of the generalizations to come.

If X is a topological space, let $\mathcal{O}(X)$ denote the lattice of open sets of X, which we can view as a poset category. Then a presheaf on X is a (contravariant) functor $\mathcal{O}(X)^{\mathrm{op}} \to \mathsf{Set}$. If $U \subseteq V$, then we have a unique arrow $U \to V$ in $\mathcal{O}(X)$, and so by functoriality any presheaf F must have a map $\rho : FV \to FU$ (called restriction), sending $f \in FV \mapsto f \restriction_U \in FU$.

Of course, where there are presheaves, there are sheaves to come, and the distinction is the following gluing condition:

Say the family $\{U_\alpha\}$ is an open cover for U, and we've selected an element x_α from each FU_α. Moreover, say these x_α are *compatible* in the sense that for any α and β, we have $x_\alpha \restriction (U_\alpha \cap U_\beta) = x_\beta \restriction (U_\alpha \cap U_\beta)$. Then we want to know that we can "glue" the x_α together into a unique $x \in FU$, so that $x_\alpha = x \restriction U_\alpha$.

It turns out the category of sheaves on a topological space (and, in the language of the coming section, of sheaves on a site) is extremely rich. It has all limits and colimits, is cartesian closed[10], and admits what is called a Subobject Classifier (which plays a central role in the logical aspects of the theory). Moreover, $\mathsf{Sh}(X)$ has an internal Natural Numbers Object, and these features conspire to let us do most mathematics inside of a sheaf category.

As an example of this richness, let's see how to formulate the sheaf cohomology functor in this more categorical language. This definition will immediately generalize to sheaf cohomology for sheaves on a site, which will give us a cohomology for the Weil conjectures.

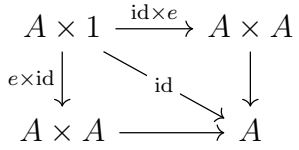
[10]Informally, this means it has "function spaces". Formally this means for every object A, the functor $- \times A : \mathsf{Sh}(X) \to \mathsf{Sh}(X)$ admits a right adjoint, written $(-)^A$.

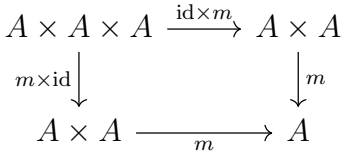
4.1 Abelian Groups Internal to a Topos

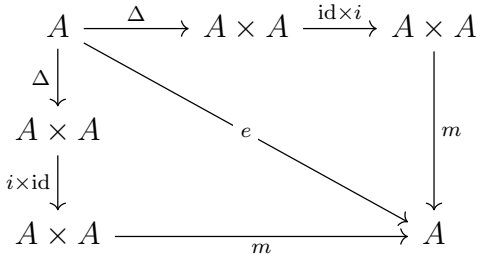
An Abelian Group Object in a category $\mathcal{C}$ is an object A equipped with

- A morhpism $e : 1 \to A$
- A morphism $m : A \times A \to A$
- A morhpism $i : A \to A$

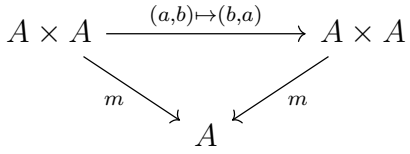
making the following diagrams commmute:







If we write $+$ for m and $-$ for i, then the first diagram expresses the familiar rules $e + x = x = x + e$ for each $x \in A$. The second expresses associativity, and the last expresses $x + (-x) = e = (-x) + x$. At this point we have a group object, and it becomes abelian upon requiring the following commute:



which expresses $a + b = b + a$.

Moreover, say we have two abelian group objects A and B inside $\mathcal{C}$. Then it's easy to see that the arrows $f : A \to B$ in $\mathcal{C}$ making the diagram

$$\begin{array}{ccc} A \times A & \xrightarrow{f \times f} & B \times B \\ {\scriptstyle m_A}\downarrow & & \downarrow{\scriptstyle m_B} \\ A & \xrightarrow[f]{} & B \end{array}$$

commute are stable under composition, and act as internal group homomorphisms. After all, this diagram exactly that $f(a_1 +_A a_2) = fa_1 +_B fa_2$.

Then there is a subcategory of $\mathcal{C}$ whose objects are the abelian group objects and whose arrows are the group homomorphisms, and we call this category $\mathbf{ab}(\mathcal{C})$. The abelian groups internal to $\mathcal{C}$.

Then one can show that for a topos $\mathsf{Sh}(X)$, the category $\mathbf{ab}(\mathsf{Sh}(X))$ is an AB5 category! Moreover, we can prove this fact using facts which will be true of toposes over sites more generally. See [9] for more.

But now we're golden! If 1 is the terminal object, then the functor $\mathrm{Hom}_{\mathsf{Sh}(X)}(1, -)$ restricts to an additive, left exact functor $\mathbf{ab}(\mathsf{Sh}(X)) \to \mathbf{ab}(\mathsf{Set})$, where, of course, $\mathbf{ab}(\mathsf{Set})$ is just the usual category of abelian groups!

Now the general theory of AB5 categories kicks in, and we get a notion of sheaf cohomology given by the derived functors of $\mathrm{Hom}_{\mathsf{Sh}(X)}(1, -)$[11].

So we know the theory works. All that is left is to give the definition of a Grothendieck Topology on a category, and show how it generalizes the idea of a topology on a space X.

4.2 A Site for Sore Eyes

Ok, so what parts of a topology did we *really* use in order to define sheaves? Well, let's fix a (small) category $\mathcal{C}$. We want objects in $\mathcal{C}$ to act like the open sets of a topological space.

We start with presheaves. These are contravariant functors $\mathcal{C}^{\mathrm{op}} \to \mathsf{Set}$. Then to define the sheaf condition we need to know what it means for a family of open sets to *cover* another open set.

Grothendieck realized that the important features are these[12]:

For each object X of $\mathcal{C}$, we pick a family $j(X)$ of subfunctors of the representable $\mathrm{Hom}_{\mathcal{C}}(-, X)$. A subfunctor R should be thought of as a collection of objects in $\mathcal{C}$ which cover X. So the family $j(X)$ gives all the possible open covers of X.

First, we require $\mathrm{Hom}_{\mathcal{C}}(-, X)$ to be in $j(X)$. That is, U should cover itself.

[11] I can't help but mentioning some examples of this in action when we look at specific toposes, even though I know we haven't actually mentioned any non-sheaf toposes in this note. In the case of $\mathsf{Sh}(X)$, we unsurprisingly recover classical sheaf cohomology. In a topos of G-sets for a group G, we get the group cohomology of G. Moreover, given two toposes $\mathcal{E}$ and $\mathcal{F}$ with a geometric morphism between them, we can get spectral sequences relating the cohomology theories of the two categories. Again, see [9] for more.

[12] For more, see [9] or [2]

Next, we require these to be pullback stable, in the sense that whenever R is a covering family for X, if we pullback as indicated in the following diagram, we again get a covering family for Y:

$$\begin{array}{ccc} R_f & \longrightarrow & R \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(-,Y) & \xrightarrow[\mathrm{Hom}_{\mathcal{C}}(-,f)]{} & \mathrm{Hom}_{\mathcal{C}}(-,X) \end{array}$$

Intuitively, if we have an open covering $\{U_\alpha\}$ for U, and we know $V \subseteq U$, then the family $\{U_\alpha \cap V\}$ should be an open covering for V.

Lastly, if we have a cover $\{U_\alpha\}$ of U, and we have covers $\{U_\alpha^\beta\}$ for each α, then the entire collection $\{U_\alpha^\beta\}$ should be a cover for U. Formally, say R is a subfunctor of $\mathrm{Hom}_{\mathcal{C}}(-,X)$, and $S \in j(X)$. Then if for each $Y \in \mathcal{C}$ and every $f \in S(Y)$ we have $R_f \in j(Y)$, we must have $R \in j(X)$.

With all this in place, we can finally define the category $\mathsf{Sh}(\mathcal{C}, j)$ to be the full subcategory of the category of presheaves on $\mathcal{C}$ (with natural transformations as arrows) consisting of those objects with the following property:

A presheaf F is a sheaf when, for every $X \in \mathcal{C}$ and $R \in j(X)$, every natural transformation $\alpha R \to F$ extends uniquely to $\mathrm{Hom}_{\mathcal{C}}(-,X)$.

$$\begin{array}{ccc} R & \longrightarrow & \mathrm{Hom}_{\mathcal{C}}(-,X) \\ \downarrow{\scriptstyle \alpha} & \swarrow & \\ F & & \end{array}$$

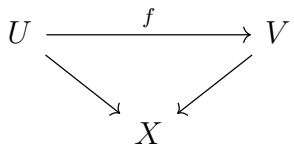
By the yoneda lemma, we know that natural transformations $\mathrm{Hom}_{\mathcal{C}}(-,X) \to F$ are in bijection with elements of $F(X)$. So then, asking for a natural transformation from $R \to F$ (where we can write R as a colimit of representables of objects with arrows into X) is like asking for an element of $F(Y)$ for each Y in the covering R. Saying that we can extend such an α to the whole of $\mathrm{Hom}_{\mathcal{C}}(-,X)$ is saying we can glue these pieces together. Which is exactly the sheaf condition.

4.3 Finally Solving the Problem

Now, let U and X be smooth varieties over an algebraically closed field. We have a notion of an Étale map $f : U \to X$, which is too technical to cover here[13], and we use it to define a topos as follows.

Let t/X be the category whose objects are etale maps $U \to X$, and whose morhpisms are the maps from $f : U \to V$ making the following diagram commute:

[13]But see the excellent [14] if you're interested in more



In such a case, the map f is automatically Étale.

Next, we define the coverings. If $\varphi_\alpha : U_\alpha \to U$ is a family of Étale maps and U is Étale over X, then the family forms a covering exactly when $\bigcup \varphi_\alpha[U_\alpha] = U$.

One can check that this forms a Grothendieck topology j on t/X, and thus that the category $\mathsf{Sh}(\mathsf{t}/X, j)$ is a topos with properties formally similar to $\mathsf{Sh}(X)$ where X is a topological space.

In particular, we now get a cohomology theory for X which has precisely the properties needed to prove all of the Weil Conjectures except the Riemann Hypothesis. For a nice survey of the "Standard Conjectures" and how they relate to a similarly formal proof of the Riemann Hypothesis, see [11]. If instead you're intrested in reading about how the problem was *actually solved* by Deligne, as well as some details about motives and the Standard Conjectures, see [15].

References

[1] Andreas Aabrandt and Vagn Lundsgaard Hansen. The circle equation over finite fields. *Quaestiones Mathematicae*, 41(5):665–674, July 2018.

[2] Francis Borceux and Francis Borceux. *Categories of sheaves*. Number 3 in Handbook of categorical algebra / Francis Borceux. Cambridge Univ. Press, Cambridge, digitally printed version edition, 2008.

[3] Alain Connes. An essay on the Riemann Hypothesis. *arXiv:1509.05576 [math]*, September 2015. arXiv: 1509.05576.

[4] Mark Goresky. Commentary on "Numbers of solutions of equations in finite fields" by André Weil. *Bulletin of the American Mathematical Society*, 55(3):327–329, April 2018.

[5] Graduate Mathematics. The rising sea: Grothendieck on simplicity and generality - Colin McLarty [2003], December 2018.

[6] Graduate Mathematics. Nonetheless one should learn the language of topos: Grothendieck... - Colin McLarty [2018], January 2019.

[7] Alexandre Grothendieck. Some aspects of homological algebra. page 120.

[8] Institute for Advanced Study. The Weil Conjectures, from Abel to Deligne - Sophie Morel, July 2017.

[9] P. T. Johnstone. *Topos theory*. Dover books on mathematics. Dover Publications, Inc, Mineola, New York, dover edition edition, 2014.

[10] Reinhardt Kiehl and Eberhard Freitag. Etale cohomology and the weil conjecture. 1988.

[11] Steven L Kleiman. The standard conjectures. *Motives (Seattle, WA, 1991)*, 55:3–20, 1994. Publisher: American Mathematical Society Providence, RI.

[12] Michel L. Lapidus. *In search of the Riemann zeros: strings, fractal membranes and noncommutative spacetimes*. American Mathematical Society, Providence, R.I, 2008. OCLC: ocn173368799.

[13] Colin McLARTY. The Uses and Abuses of the History of Topos Theory. *The British Journal for the Philosophy of Science*, 41(3):351–375, 1990.

[14] J S Milne. Lectures on etale cohomology. page 202.

[15] James Milne. The Riemann Hypothesis over Finite Fields: From Weil to the Present Day. *arXiv:1509.00797 [math]*, September 2015. arXiv: 1509.00797.

[16] Frans Oort. The Weil Conjectures. *Nieuw Archief voor Wiskunde*, Serie 5:211, September 2014.

[17] Brian Osserman. A CONCISE ACCOUNT OF THE WEIL CONJECTURES AND ETALE COHOMOLOGY. page 6.

[18] Sam Raskin. THE WEIL CONJECTURES FOR CURVES. page 20.

[19] Richard E. BORCHERDS. Weil conjectures 1 Introduction, October 2020.

[20] Richard E. BORCHERDS. Weil conjectures 3: Riemann hypothesis, October 2020.

[21] Margaret M Robinson. THE WEIL ZETA FUNCTION AND THE IGUSA LOCAL ZETA FUNCTION. page 22.

[22] Charles A. Weibel. *An Introduction to Homological Algebra*. Cambridge University Press, 1 edition, April 1994.