

# Arithmetic Geometry and Stacky Curves

Andrew J. Kobin

`ajkobin@emory.edu`

Algebra & Number Theory Seminar

September 12, 2023



EMORY  
UNIVERSITY

## Introduction

Believe women.

Believe your colleagues.

Stop the cruelty.

## Generalized Fermat Equations

**Motivation:** Find all integer solutions  $(x, y, z)$  to the generalized Fermat equation

$$Ax^p + Bx^q = Cz^r$$

for  $A, B, C \in \mathbb{Z}$  and  $p, q, r \geq 2$ .

## Generalized Fermat Equations

**Motivation:** Find integer solutions to  $Ax^p + Bx^q = Cz^r$ .

Example  $((A, B, C) = (1, 1, 1), (p, q, r) = (2, 2, 2))$

Famously, there are infinitely many integer solutions to  $x^2 + y^2 = z^2$ , with primitive ( $\gcd(x, y, z) = 1$ ) solutions parametrized by

$$(x, y, z) = \left( \frac{s^2 - t^2}{2}, st, \frac{s^2 + t^2}{2} \right) \quad \text{for odd, coprime } s > t \geq 1.$$

## Generalized Fermat Equations

**Motivation:** Find integer solutions to  $Ax^p + Bx^q = Cz^r$ .

Example  $((A, B, C) = (1, 1, 1), (p, q, r) = (2, 2, 2))$

Famously, there are infinitely many integer solutions to  $x^2 + y^2 = z^2$ , with primitive ( $\gcd(x, y, z) = 1$ ) solutions parametrized by

$$(x, y, z) = \left( \frac{s^2 - t^2}{2}, st, \frac{s^2 + t^2}{2} \right) \quad \text{for odd, coprime } s > t \geq 1.$$



P.  
@p\_blade\_

Wow. Another day as an adult without using the Pythagorean Theorem.

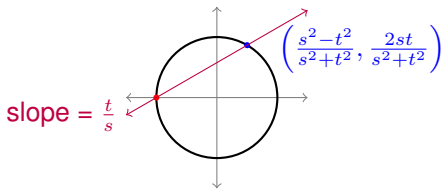
## Generalized Fermat Equations

**Motivation:** Find integer solutions to  $Ax^p + Bx^q = Cz^r$ .

**Example**  $((A, B, C) = (1, 1, 1), (p, q, r) = (2, 2, 2))$

Famously, there are infinitely many integer solutions to  $x^2 + y^2 = z^2$ , with primitive ( $\gcd(x, y, z) = 1$ ) solutions parametrized by

$$(x, y, z) = \left( \frac{s^2 - t^2}{2}, st, \frac{s^2 + t^2}{2} \right) \quad \text{for odd, coprime } s > t \geq 1.$$



## Generalized Fermat Equations

**Motivation:** Find integer solutions to  $Ax^p + Bx^q = Cz^r$ .

Example  $((A, B, C) = (1, 1, 1), (p, q, r) = (n, n, n))$

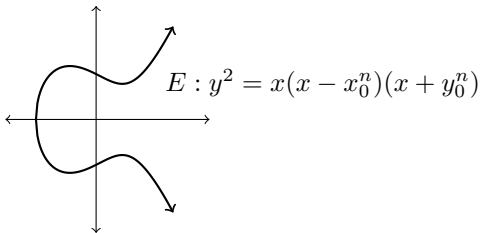
Also famously, there are *no* integer solutions to  $x^n + y^n = z^n$  for  $n > 2$ .

## Generalized Fermat Equations

**Motivation:** Find integer solutions to  $Ax^p + Bx^q = Cz^r$ .

Example  $((A, B, C) = (1, 1, 1), (p, q, r) = (n, n, n))$

Also famously, there are *no* integer solutions to  $x^n + y^n = z^n$  for  $n > 2$ . Assume  $n$  is prime. If  $(x_0, y_0, z_0)$  were such a solution, it would determine an elliptic curve



Ribet showed  $E$  is not modular. However, Wiles showed all such elliptic curves are modular, a contradiction.



## Generalized Fermat Equations

**Takeaway:** Integer solutions to  $Ax^p + Bx^q = Cz^r$  can be studied using geometry.

## Generalized Fermat Equations

Here are some more known cases of  $Ax^p + Bx^q = Cz^r$ .

- (Beukers, Darmon–Granville) Let  $\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1$ . The equation  $x^p + y^q = z^r$  has infinitely many primitive solutions when  $\chi > 0$  and finitely many when  $\chi < 0$ .

## Generalized Fermat Equations

Here are some more known cases of  $Ax^p + Bx^q = Cz^r$ .

- (Beukers, Darmon–Granville) Let  $\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1$ . The equation  $x^p + y^q = z^r$  has infinitely many primitive solutions when  $\chi > 0$  and finitely many when  $\chi < 0$ .
- (Mordell, Zagier, Edwards) When  $\chi > 0$ , the primitive solutions to  $x^p + y^q = z^r$  may always be parametrized explicitly (as in the (2, 2, 2) case).
- (Fermat, Euler, et al.) The case  $\chi = 0$  only occurs for (2, 3, 6), (4, 4, 2), (3, 3, 3) and permutations of these. In each case, descent proves there are finitely many primitive solutions.
- (2, 3, 7) was solved by Poonen–Schaeffer–Stoll (2007).
- (2, 3, 8), (2, 3, 9) were solved by Bruin (1999, 2004).
- etc.

## Generalized Fermat Equations

**Question:** How do we count solutions to such equations?

## Generalized Fermat Equations

**Question:** How do we count solutions to such equations?

One strategy is to form the scheme theoretic locus of nontrivial, primitive solutions in 3-dimensional space over  $\mathbb{Z}$ :

$$S = \text{Spec}(\mathbb{Z}[x, y, z]/(Ax^p + By^q - Cz^r)) \setminus \{x = y = z = 0\} \subseteq \mathbb{A}_{\mathbb{Z}}^3.$$

For any ring  $R$ , this keeps track of the  $R$ -solutions:

$$S(R) = \{x, y, z \in R \mid Ax^p + By^q = Cz^r, \text{ nontrivial, primitive}\}.$$

## Generalized Fermat Equations

$$S = \text{Spec}(\mathbb{Z}[x, y, z]/(Ax^p + By^q - Cz^r)) \setminus \{x = y = z = 0\} \subseteq \mathbb{A}_{\mathbb{Z}}^3$$

Let  $G$  be the group of symmetries of  $S$ . ( $G = \mathbb{G}_m \cdot (\mu_p \times \mu_q \times \mu_r)$ )

## Generalized Fermat Equations

$$S = \text{Spec}(\mathbb{Z}[x, y, z]/(Ax^p + By^q - Cz^r)) \setminus \{x = y = z = 0\} \subseteq \mathbb{A}_{\mathbb{Z}}^3$$

Let  $G$  be the group of symmetries of  $S$ . ( $G = \mathbb{G}_m \cdot (\mu_p \times \mu_q \times \mu_r)$ )

We can form the quotient  $X = S/G$  whose points are exactly the equivalence classes of solutions:

$$X(R) = \{x, y, z \in R \mid Ax^p + By^q = Cz^r, \text{ nontriv., prim.}\} / \sim$$

where  $g \cdot (x, y, z) \sim (x, y, z)$ .

Upside: these are easier to count than  $S(R)$ .

Downside: the geometry of  $X$  is bad!

## Generalized Fermat Equations

$$S = \text{Spec}(\mathbb{Z}[x, y, z]/(Ax^p + By^q - Cz^r)) \setminus \{x = y = z = 0\} \subseteq \mathbb{A}_{\mathbb{Z}}^3$$

Let  $G$  be the group of symmetries of  $S$ . ( $G = \mathbb{G}_m \cdot (\mu_p \times \mu_q \times \mu_r)$ )

We can form the quotient **stack**  $\mathcal{X} = [S/G]$  whose points are exactly the **groupoid** of solutions:

$\mathcal{X}(R)$  : objects: nontriv., prim. solutions to  $Ax^p + By^q = Cz^r$

morphisms:  $(x, y, z) \xrightarrow{g} g \cdot (x, y, z)$ .

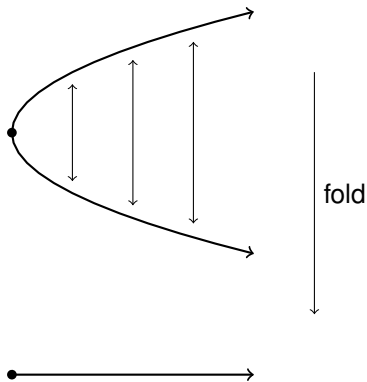
Upside: these are easier to count than  $S(R)$ .

Downside: **none - stacks are awesome!**



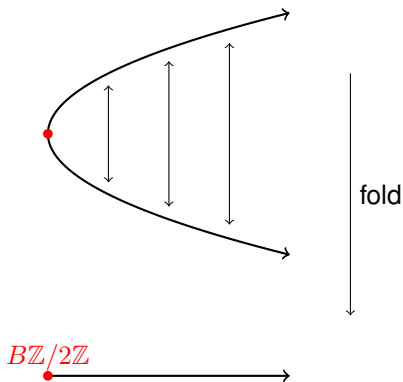
# Stacks

**Problem:** all sorts of information is lost when we consider quotients.



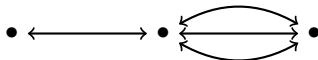
## Stacks

**Solution:** Keep track of extra automorphisms using *groupoids*.

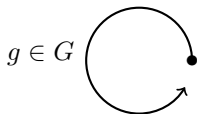


# Stacks

A groupoid is a category with only isomorphisms.

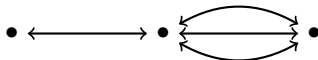


Main example: for a group  $G$ ,  $BG$  has one object  $\bullet$  and one morphisms for every  $g \in G$ :

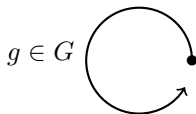


# Stacks

A groupoid is a category with only isomorphisms.



Main example: for a group  $G$ ,  $BG$  has one object  $\bullet$  and one morphism for every  $g \in G$ :



A stack is a functor  $\mathcal{X} : \text{Ring} \rightarrow \text{Groupoid}$  that assigns to each ring  $R$  a groupoid  $\mathcal{X}(R)$ .

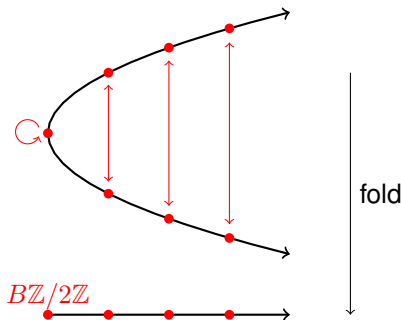
Moreover, it must satisfy *descent*: for any cover\*  $\{R \rightarrow S_i\}$ , the objects/morphisms of  $\mathcal{X}(R)$  are determined by those of  $\{\mathcal{X}(S_i)\}$ .

## Stacks

A stack is a functor  $\mathcal{X} : \text{Ring} \rightarrow \text{Groupoid}$  satisfying descent.

### Example

For our plane curve  $X : y^2 = x$ , groupoids remember automorphisms like  $(x, y) \leftrightarrow (x, -y)$



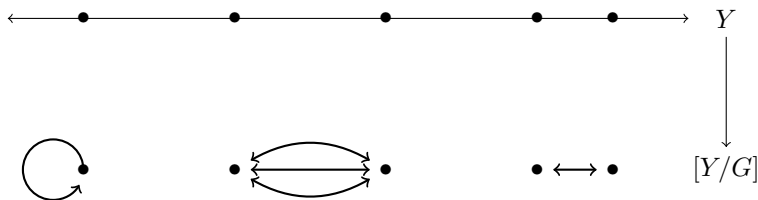
Here, each downstairs “point” is obtained by collapsing upstairs points together and identifying morphisms.

# Stacks

A stack is a functor  $\mathcal{X} : \text{Ring} \rightarrow \text{Groupoid}$  satisfying descent.

## Example

More generally, for a group  $G$  acting on a space  $Y$ , we can form the *quotient stack*  $[Y/G]$  whose  $R$ -points are the groupoid of  $G$ -orbits:



Special case:  $[*/G] = BG$ .

# Stacky Curves

Here's a technical definition of a stacky curve:

## Definition

A **stacky curve** is a smooth, separated, connected stack  $\mathcal{X} : \text{Ring} \rightarrow \text{Groupoid}$  satisfying:

- 1  $\mathcal{X}$  has an underlying *coarse moduli scheme*  $X$  with a map  $\pi : \mathcal{X} \rightarrow X$  (collapse the groupoid to a set).
- 2  $\pi$  is an isomorphism away from a finite set of points.
- 3  $X$  is 1-dimensional (aka a curve).
- 4 There is an étale surjection  $U \rightarrow \mathcal{X}$  where  $U$  is a scheme.
- 5 The diagonal  $\Delta_{\mathcal{X}} : \mathcal{X} \rightarrow \mathcal{X} \times \mathcal{X}$  is representable.

## Stacky Curves

Here's a more informal definition though:

A stacky curve  $\mathcal{X}$  consists of an ordinary curve  $X$ , together with a finite number of marked points  $P_1, \dots, P_n$ , each of which is decorated with a finite automorphism group  $G_i$ .

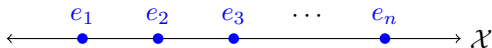


# Stacky Curves

Here's a more informal definition though:

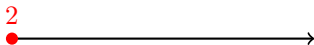
A stacky curve  $\mathcal{X}$  consists of an ordinary curve  $X$ , together with a finite number of marked points  $P_1, \dots, P_n$ , each of which is decorated with a finite automorphism group  $G_i$ .

Over  $\mathbb{C}$  (or  $\mathbb{Q}$ , or a number field), the groups  $G_i$  are cyclic, so  $G_i \cong \mathbb{Z}/e_i\mathbb{Z}$  and we can keep track of this data with a cartoon like this:



# Stacky Curves

Here's a cartoon of our folded parabola:



# Stacky Curves

Here's a cartoon of a stacky curve with coarse space  $\mathbb{P}^1$ :



# Stacky Curves

Here's a cartoon of our stacky curve  $[S/G]$ , where  $S =$  primitive integer solutions to  $Ax^p + Bx^q = Cz^r$ :



## Generalized Fermat Equations, Revisited

To find solutions to  $Ax^p + Bx^q = Cz^r$ , we can exploit the geometry of  $\mathcal{X} = [S/G]$ :

## Generalized Fermat Equations, Revisited

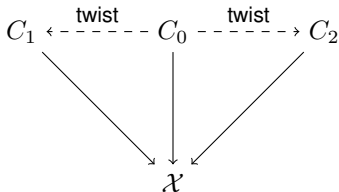
To find solutions to  $Ax^p + Bx^q = Cz^r$ , we can exploit the geometry of  $\mathcal{X} = [S/G]$ :

$$\begin{array}{c} C_0 \\ \downarrow \\ \mathcal{X} \end{array}$$

(1) Find a nice map  $C_0 \rightarrow \mathcal{X}$  from a curve  $C_0$  whose points are easy to find (e.g. a conic).

## Generalized Fermat Equations, Revisited

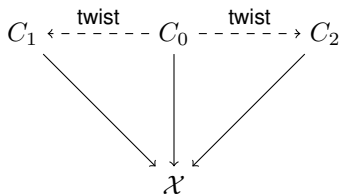
To find solutions to  $Ax^p + Bx^q = Cz^r$ , we can exploit the geometry of  $\mathcal{X} = [S/G]$ :



- (1) Find a nice map  $C_0 \rightarrow \mathcal{X}$  from a curve  $C_0$  whose points are easy to find (e.g. a conic).
- (2) Compute all twists of  $C_0$  and their points.

## Generalized Fermat Equations, Revisited

To find solutions to  $Ax^p + Bx^q = Cz^r$ , we can exploit the geometry of  $\mathcal{X} = [S/G]$ :



- (1) Find a nice map  $C_0 \rightarrow \mathcal{X}$  from a curve  $C_0$  whose points are easy to find (e.g. a conic).
- (2) Compute all twists of  $C_0$  and their points.
- (3) Use descent to identify points on  $\mathcal{X}$ .



## Generalized Fermat Equations, Revisited

### Example

For  $\mathcal{X} : x^2 + y^2 = z^2$ , there is an étale map

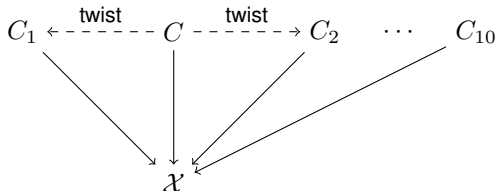
$$\begin{array}{c} \mathbb{P}^1 \\ \downarrow \\ \mathcal{X} \end{array}$$

and  $\mathbb{P}^1$  has infinitely many points which descend, so there are infinitely many primitive Pythagorean triples.

## Generalized Fermat Equations, Revisited

## Example (Poonen–Schaeffer–Stoll)

For  $\mathcal{X} : x^2 + y^3 = z^7$ , there is an étale map



where  $C$  is the Klein quartic, defined by  $x^3y + y^3 + x = 0$ . Descending points from  $C$  and its 10 twists gives 16 primitive solutions:

$$\begin{aligned}
 &(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad (0, \pm 1, \pm 1), \quad (\pm 3, -2, 1), \\
 &(\pm 71, -17, 2), \quad (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113), \\
 &(\pm 21063928, -76271, 17).
 \end{aligned}$$

## Local-Global Principle for Algebraic Curves

The classic local-global principle for an algebraic curve  $X$  asks if  $X(\mathbb{Q}) \neq \emptyset$  is equivalent to  $X(\mathbb{Q}_p) \neq \emptyset$  for all completions  $\mathbb{Q}_p$ ,  $p \leq \infty$ .

## Local-Global Principle for Algebraic Curves

The classic local-global principle for an algebraic curve  $X$  asks if  $X(\mathbb{Q}) \neq \emptyset$  is equivalent to  $X(\mathbb{Q}_p) \neq \emptyset$  for all completions  $\mathbb{Q}_p$ ,  $p \leq \infty$ .

Let  $g = g(X)$  be the genus of  $X$ . It is known that:

- (Hasse–Minkowski) If  $g = 0$ , the LGP holds for  $X$ .
- There are counterexamples to the LGP for all  $g > 0$ .  
For example,  $X : 2y^2 = 1 - 17x^4$ .

## Local-Global Principle for Stacky Curves

For a stacky curve  $\mathcal{X}$ , we pose the *local-global principle for integral points*:

is  $\mathcal{X}(\mathbb{Z}) \neq \emptyset$  equivalent to  $\mathcal{X}(\mathbb{Z}_p) \neq \emptyset$  for all completions  $\mathbb{Z}_p$ ?

## Local-Global Principle for Stacky Curves

For a stacky curve  $\mathcal{X}$ , we pose the *local-global principle for integral points*:

is  $\mathcal{X}(\mathbb{Z}) \neq \emptyset$  equivalent to  $\mathcal{X}(\mathbb{Z}_p) \neq \emptyset$  for all completions  $\mathbb{Z}_p$ ?

This time, the genus  $g = g(\mathcal{X})$  can be *rational*:

$$g(\mathcal{X}) = g(X) + \frac{1}{2} \sum_{i=1}^n \frac{e_i - 1}{e_i}$$

where  $X$  is the coarse space and  $e_1, \dots, e_n$  are the orders of the automorphisms groups at the finite number of stacky points.

When  $\mathcal{X}$  is a *wild* stacky curve, I proved a more general formula for  $g(\mathcal{X})$ .

## Local-Global Principle for Stacky Curves

### Example

Our cartoon from before is a stacky curve with genus

$$g = \frac{1}{2} \left( \frac{15}{16} + \frac{4}{5} + \frac{2}{3} + \frac{59}{60} \right) = \frac{271}{160}.$$



### Example

Our stacky curve  $[S/G]$ , where  $S =$  primitive integer solutions to

$$Ax^p + Bx^q = Cz^r, \text{ has genus } g = \frac{1}{2} \left( 3 - \frac{1}{p} - \frac{1}{q} - \frac{1}{r} \right).$$



For example, the  $(2, 3, 7)$  curve has genus  $g = \frac{85}{84}$ .

## Local-Global Principle for Stacky Curves

For  $\mathcal{X} = [S/G]$  where  $S : Ax^p + By^q = Cz^r$ ,  $g = \frac{1}{2} \left( 3 - \frac{1}{p} - \frac{1}{q} - \frac{1}{r} \right)$ .

### Theorem (Bhargava–Poonen)

- ① *If  $g < \frac{1}{2}$ , the LGP holds.*
- ② *There are counterexamples to the LGP when  $g = \frac{1}{2}$ .*

### Theorem (Darmon–Granville)

*In the  $(2, 2, n)$  case, with  $g = \frac{n-1}{n}$ , there are counterexamples to the LGP.*

Joint work with Duque-Rosero, Keyes, Roy, Sankar, Wang (in progress): a complete solution in the  $(2, 2, n)$  case.



## Another Example of a Stacky Curve

Here's another important stacky curve:



**Fact:**  $\mathcal{X}(1) \cong \overline{\mathcal{M}}_{1,1}$ , the compactified moduli stack of elliptic curves.

# Another Example of a Stacky Curve

Here's another important stacky curve:

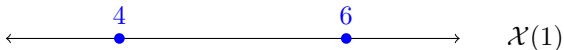


**Fact:**  $\mathcal{X}(1) \cong \overline{\mathcal{M}}_{1,1}$ , the compactified moduli stack of elliptic curves.



## Another Example of a Stacky Curve

Here's another important stacky curve:



**Fact:**  $\mathcal{X}(1) \cong \overline{\mathcal{M}}_{1,1}$ , the compactified moduli stack of elliptic curves.

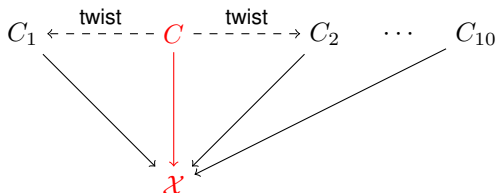
More generally, there are modular curves  $\mathcal{X}(N)$ ,  $\mathcal{X}_0(N)$ ,  $\mathcal{X}_1(N)$ , etc. parametrizing elliptic curves with *level structure*.

Enough about those for now, but remember the Klein quartic?

## Generalized Fermat Equations, Revisited

## Example (Poonen–Schaeffer–Stoll)

For  $\mathcal{X} : x^2 + y^3 = z^7$ , there is an étale map

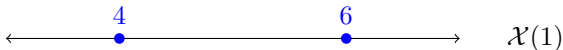


where  $C$  is the Klein quartic, defined by  $x^3y + y^3 + x = 0$ . Descending points from  $C$  and its 10 twists gives 16 primitive solutions:

$$\begin{aligned}
 &(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad (0, \pm 1, \pm 1), \quad (\pm 3, -2, 1), \\
 &(\pm 71, -17, 2), \quad (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113), \\
 &(\pm 21063928, -76271, 17).
 \end{aligned}$$

## Another Example of a Stacky Curve

Here's another important stacky curve:



**Fact:**  $\mathcal{X}(1) \cong \overline{\mathcal{M}}_{1,1}$ , the compactified moduli stack of elliptic curves.

More generally, there are modular curves  $\mathcal{X}(N)$ ,  $\mathcal{X}_0(N)$ ,  $\mathcal{X}_1(N)$ , etc. parametrizing elliptic curves with *level structure*.

Enough about those for now, but remember the Klein quartic? It's secretly isomorphic to  $\mathcal{X}(7)$ .

## Another Example of a Stacky Curve

Here's another important stacky curve:



**Fact:**  $\mathcal{X}(1) \cong \overline{\mathcal{M}}_{1,1}$ , the compactified moduli stack of elliptic curves.

**Fact 2:** Modular curves give rise to *modular forms*.



## Modular Forms

Let  $\mathfrak{h} = \{z \in \mathbb{C} : \text{im}(z) > 0\}$  be the upper half-plane in  $\mathbb{C}$ .

### Definition

A **modular form** of weight  $2k$  is a holomorphic function  $f : \mathfrak{h} \rightarrow \mathbb{C}$  such that

- 1 For all  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ ,  $f(z) = (cz + d)^{-2k} f(gz)$ .
- 2  $f$  is holomorphic at  $\infty$ .

## Modular Forms

Let  $\mathfrak{h} = \{z \in \mathbb{C} : \text{im}(z) > 0\}$  be the upper half-plane in  $\mathbb{C}$ .

### Definition

A **modular form** of weight  $2k$  is a holomorphic function  $f : \mathfrak{h} \rightarrow \mathbb{C}$  such that

- 1 For all  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ ,  $f(z) = (cz + d)^{-2k} f(gz)$ .
- 2  $f$  is holomorphic at  $\infty$ .

Informal version: modular forms are highly symmetric holomorphic functions on the upper half-plane in  $\mathbb{C}$ .





## Modular Forms

Given a modular form  $f : \mathfrak{h} \rightarrow \mathbb{C}$ , we can define a differential form  $\omega = f(z) dz^k$ .

By the symmetry of  $f$ ,  $\omega$  is not just defined on the upper half-plane, but on the quotient  $\mathfrak{h}/SL_2(\mathbb{Z})$ .

Compactifying by adding a point at  $\infty$ , this quotient  $\overline{\mathfrak{h}/SL_2(\mathbb{Z})}$  becomes isomorphic to  $\mathcal{X}(1)$ , the moduli stack of elliptic curves.

Upshot: modular forms act like “functions” on the moduli stack  $\mathcal{X}(1)$ .

## Modular Forms Mod $p$

This allows one to define modular forms over any field  $k$ , as differential forms on the moduli stack  $\mathcal{X}(1)$  of elliptic curves over  $k$ .

Joint work with D. Zureick-Brown (in progress): describe the space of mod  $p$  modular forms using the stacky structure of  $\mathcal{X}(1)$  and other modular curves over  $\mathbb{F}_p$ .

## Modular Forms Mod $p$

This allows one to define modular forms over any field  $k$ , as differential forms on the moduli stack  $\mathcal{X}(1)$  of elliptic curves over  $k$ .

Joint work with D. Zureick-Brown (in progress): describe the space of mod  $p$  modular forms using the stacky structure of  $\mathcal{X}(1)$  and other modular curves over  $\mathbb{F}_p$ .

For  $p > 3$ , the story for  $\mathcal{X}(1)$  is the same as before:



However, over  $\mathbb{F}_2$  and  $\mathbb{F}_3$ , the stacky structure of  $\mathcal{X}(1)$  looks different:



Thank you!