Stacky Curves and Generalized Fermat Equations

Andrew J. Kobin

ajkobin@emory.edu

Rethinking Number Theory @ AWM Symposium

October 1, 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

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

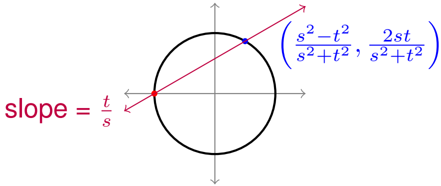
Generalized Fermat Equations

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

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



Generalized Fermat Equations

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

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

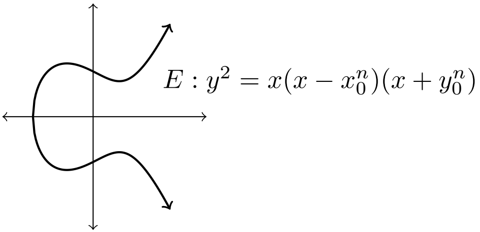
Also famously, there are *no* integer solutions to $x^n + y^n = z^n$ for $n > 2$.

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 surface of (primitive, nontrivial) solutions in 3-dimensional space over $\mathbb{Z}$:

$$S = \{(x, y, z) \in \mathbb{Z}^3 \mid Ax^p + By^q = Cz^r, \text{ nontrivial, primitive}\} \subseteq \mathbb{A}^3_{\mathbb{Z}}.$$

Generalized Fermat Equations

$$S = \{(x, y, z) \in \mathbb{Z}^3 \mid Ax^p + By^q = Cz^r, \text{ nontrivial, primitive}\}$$

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

$$S = \{(x,y,z) \in \mathbb{Z}^3 \mid Ax^p + By^q = Cz^r, \text{ nontrivial, primitive}\}$$

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 curve $X = S/G$ whose points are exactly the equivalence classes of solutions:

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

Upside: these are easier to count than $S(\mathbb{Z})$.
Downside: the geometry of X is bad!

Generalized Fermat Equations

$S = \{(x, y, z) \in \mathbb{Z}^3 \mid Ax^p + By^q = Cz^r,$ nontrivial, primitive$\}$

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 **stacky** curve $\mathcal{X} = [S/G]$ whose points **remember the symmetries of each solution**:

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

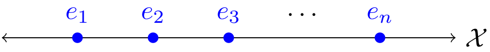
morphisms: $(x, y, z) \xrightarrow{g} g \cdot (x, y, z)$.

Upside: these are easier to count than $S(\mathbb{Z})$.
Downside: **none - stacks are awesome!**

Stacky Curves

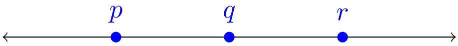
Here's an informal definition of a stacky curve:

A stacky curve $\mathcal{X}$ consists of an ordinary curve X, together with a finite number of marked points $P_1, \ldots, P_n$, each of which is decorated with a number $e_i =$ order of the group of symmetries of P_i.



Stacky Curves

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

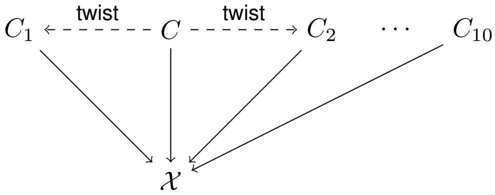


Generalized Fermat Equations, Revisited

To solve $Ax^p + Bx^q = Cz^r$, exploit the geometry of $\mathcal{X} = [S/G]$.

Example (Poonen–Schaeffer–Stoll ('07))

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:

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad (0, \pm 1, \pm 1), \quad (\pm 3, -2, 1),$$
$$(\pm 71, -17, 2), \quad (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113),$$
$$(\pm 21063928, -76271, 17).$$

Local-Global Principle for Curves

For a curve X, the *local-global principle* says that:

X having $\mathbb{Q}$-points is equivalent to X having $\mathbb{Q}_p$-points for all p.

Local-Global Principle for Curves

For a curve X, the *local-global principle* says that:

X having $\mathbb{Q}$-points is equivalent to X having $\mathbb{Q}_p$-points for all p.

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** $\mathcal{X}$, the *local-global principle* says that:

$\mathcal{X}$ having $\mathbb{Z}$-points is equivalent to $\mathcal{X}$ having $\mathbb{Z}_p$-points for all p.

Local-Global Principle for Stacky Curves

For a **stacky curve** $\mathcal{X}$, the *local-global principle* says that:

$\mathcal{X}$ having $\mathbb{Z}$-points is equivalent to $\mathcal{X}$ having $\mathbb{Z}_p$-points for all p.

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

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

Local-Global Principle for Stacky Curves

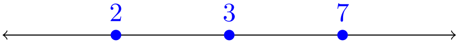
For a **stacky curve** $\mathcal{X}$, the *local-global principle* says that:

> $\mathcal{X}$ having $\mathbb{Z}$-points is equivalent to $\mathcal{X}$ having $\mathbb{Z}_p$-points for all p.

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

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

Example



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

Local-Global Principle for Stacky Curves

For a **stacky curve** $\mathcal{X}$, the *local-global principle* says that:

$\mathcal{X}$ having $\mathbb{Z}$-points is equivalent to $\mathcal{X}$ having $\mathbb{Z}_p$-points for all p.

Theorem (Bhargava–Poonen ('20))

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

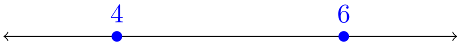
Theorem (Darmon–Granville ('95))

When $g = \frac{n-1}{n}$, there are counterexamples to the LGP coming from the generalized Fermat equation with exponents $(2, 2, n)$.

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:

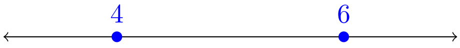


$\mathcal{X}(1)$

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:



$\mathcal{X}(1)$

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

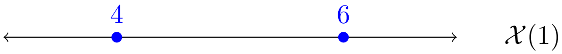
Modular Forms Mod p

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

Modular Forms Mod p

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

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



and $\bigoplus \mathcal{M}_k \cong \mathbb{F}_p[x_4, x_6]$ (originally due to Edixhoven).

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

Theorem (Deligne ('72), K.–Zureick-Brown ('23+ϵ))

For $p = 2, 3$, the ring of modular forms mod p is $\mathbb{F}_p[x_1, x_6]$.

Thank you!

Questions?