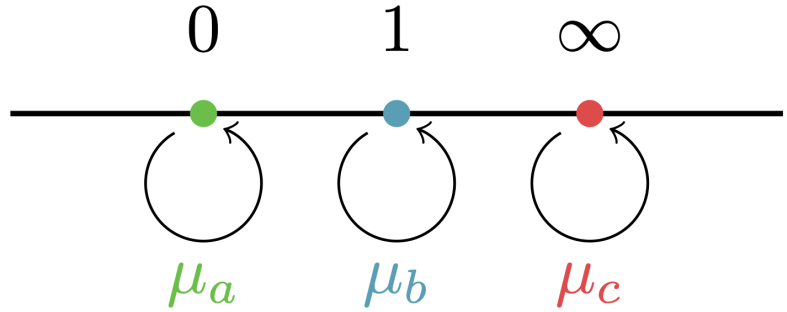
Generalized Fermat equations, stacky curves, and asymptotics

PhD defense

Santiago Arango-Piñeros

Emory University

April 3, 2025



I did four things:

1. Reinterpreted a two classical theorems in the theory of GFE from the point of view of the method of descent on stacky curves.
2. Counted primitive integral solutions to spherical GFEs.
3. Counted rational points on certain stacks associated to the GFE $x^2 + y^2 = z^c$.
4. Counted the number of isomorphism classes of 5-isogenies of elliptic curves defined over $\mathbb{Q}$ and bounded naive height (with Han, Padurariu, and Park).

I did four things:

1. Reinterpreted a two classical theorems in the theory of GFE from the point of view of the method of descent on stacky curves.
2. Counted primitive integral solutions to spherical GFEs.
3. Counted rational points on certain stacks associated to the GFE $x^2 + y^2 = z^c$.
4. Counted the number of isomorphism classes of 5-isogenies of elliptic curves defined over $\mathbb{Q}$ and bounded naive height (with Han, Padurariu, and Park).

I did four things:

1. Reinterpreted a two classical theorems in the theory of GFE from the point of view of the method of descent on stacky curves.
2. Counted primitive integral solutions to spherical GFEs.
3. Counted rational points on certain stacks associated to the GFE $x^2 + y^2 = z^c$.
4. Counted the number of isomorphism classes of 5-isogenies of elliptic curves defined over $\mathbb{Q}$ and bounded naive height (with Han, Padurariu, and Park).

I did four things:

1. Reinterpreted a two classical theorems in the theory of GFE from the point of view of the method of descent on stacky curves.
2. Counted primitive integral solutions to spherical GFEs.
3. Counted rational points on certain stacks associated to the GFE $x^2 + y^2 = z^c$.
4. Counted the number of isomorphism classes of 5-isogenies of elliptic curves defined over $\mathbb{Q}$ and bounded naive height (with Han, Padurariu, and Park).

I did four things:

1. Reinterpreted a two classical theorems in the theory of GFE from the point of view of the method of descent on stacky curves.
2. Counted primitive integral solutions to spherical GFEs.
3. Counted rational points on certain stacks associated to the GFE $x^2 + y^2 = z^c$.
4. Counted the number of isomorphism classes of 5-isogenies of elliptic curves defined over $\mathbb{Q}$ and bounded naive height (with Han, Padurariu, and Park).

I did four things:

1. Reinterpreted a two classical theorems in the theory of GFE from the point of view of the method of descent on stacky curves.
2. Counted primitive integral solutions to spherical GFEs.
3. Counted rational points on certain stacks associated to the GFE $x^2 + y^2 = z^c$.
4. Counted the number of isomorphism classes of 5-isogenies of elliptic curves defined over $\mathbb{Q}$ and bounded naive height (with Han, Padurariu, and Park).

Motivation: Fermat equations

$F := x^n + y^n - z^n$, for some $n \geqslant 2$.

A triple $(x, y, z) \in \mathbb{Z}$ is a primitive solution if $F(x, y, z) = 0$ and there is no prime p dividing x, y, and z.

The (orbifold) Euler characteristic of F is $\chi := \frac{3}{n} - 1$.

Euler characteristic	$\chi > 0$	$\chi = 0$	$\chi < 0$
Degree	$n = 2$	$n = 3$	$n > 3$
Number of primitive solutions	∞	6	$\leqslant 8$

Motivation: Fermat equations

$F := x^n + y^n - z^n$, for some $n \geqslant 2$.

A triple $(x, y, z) \in \mathbb{Z}$ is a primitive solution if $F(x, y, z) = 0$ and there is no prime p dividing x, y, and z.

The (orbifold) Euler characteristic of F is $\chi := \frac{3}{n} - 1$.

Euler characteristic	$\chi > 0$	$\chi = 0$	$\chi < 0$
Degree	$n = 2$	$n = 3$	$n > 3$
Number of primitive solutions	∞	6	$\leqslant 8$

Motivation: Fermat equations

$F := x^n + y^n - z^n$, for some $n \geqslant 2$.

A triple $(x, y, z) \in \mathbb{Z}$ is a primitive solution if $F(x, y, z) = 0$ and there is no prime p dividing x, y, and z.

The (orbifold) Euler characteristic of F is $\chi := \frac{3}{n} - 1$.

Euler characteristic	$\chi > 0$	$\chi = 0$	$\chi < 0$
Degree	$n = 2$	$n = 3$	$n > 3$
Number of primitive solutions	∞	6	$\leqslant 8$

Motivation: Fermat equations

$F := x^n + y^n - z^n$, for some $n \geqslant 2$.

A triple $(x, y, z) \in \mathbb{Z}$ is a primitive solution if $F(x, y, z) = 0$ and there is no prime p dividing x, y, and z.

The (orbifold) Euler characteristic of F is $\chi := \frac{3}{n} - 1$.

Euler characteristic	$\chi > 0$	$\chi = 0$	$\chi < 0$
Degree	$n = 2$	$n = 3$	$n > 3$
Number of primitive solutions	∞	6	$\leqslant 8$

Pythagorean triples ($\chi > 0$)

$$\phi(s,t) := (s^2 - t^2, 2st, s^2 + t^2), \quad \hat{\phi}(s,t) := (2st, s^2 - t^2, s^2 + t^2).$$

Theorem (300 BCE)

Every primitive integral solution (x, y, z) to the Diophantine equation $x^2 + y^2 = z^2$ corresponds to

$$\phi(s,t), \quad -\phi(s,t), \quad \hat{\phi}(s,t), \quad -\hat{\phi}(s,t),$$

for a unique pair of tuples $\pm(s,t) \in \mathbb{Z}^2$ satisfying $\gcd(s,t) = 1$ and $s \not\equiv t \mod 2$.

Example

$(3,4,5)$ satisfies $3^2 + 4^2 = 5^2$ and corresponds to $\phi(\pm(2,1))$.

$(6,8,10)$ satisfies $6^2 + 8^2 = 10^2$ but it is not primitive since 2 divides $6, 8$, and 10.

Pythagorean triples ($\chi > 0$)

$$\phi(s,t) := (s^2 - t^2, 2st, s^2 + t^2), \quad \hat{\phi}(s,t) := (2st, s^2 - t^2, s^2 + t^2).$$

Theorem (300 BCE)

Every primitive integral solution (x, y, z) *to the Diophantine equation* $x^2 + y^2 = z^2$ *corresponds to*

$$\phi(s,t), \quad -\phi(s,t), \quad \hat{\phi}(s,t), \quad -\hat{\phi}(s,t),$$

for a unique pair of tuples $\pm(s,t) \in \mathbb{Z}^2$ *satisfying* $\gcd(s,t) = 1$ *and* $s \not\equiv t \mod 2$.

Example

$(3,4,5)$ satisfies $3^2 + 4^2 = 5^2$ and corresponds to $\phi(\pm(2,1))$.

$(6,8,10)$ satisfies $6^2 + 8^2 = 10^2$ but it is not primitive since 2 divides $6, 8$, and 10.

Pythagorean triples ($\chi > 0$)

$$\phi(s,t) := (s^2 - t^2, 2st, s^2 + t^2), \quad \hat{\phi}(s,t) := (2st, s^2 - t^2, s^2 + t^2).$$

Theorem (300 BCE)

Every primitive integral solution (x, y, z) *to the Diophantine equation* $x^2 + y^2 = z^2$ *corresponds to*

$$\phi(s,t), \quad -\phi(s,t), \quad \hat{\phi}(s,t), \quad -\hat{\phi}(s,t),$$

for a unique pair of tuples $\pm(s,t) \in \mathbb{Z}^2$ *satisfying* $\gcd(s,t) = 1$ *and* $s \not\equiv t \mod 2$.

Example

$(3,4,5)$ satisfies $3^2 + 4^2 = 5^2$ and corresponds to $\phi(\pm(2,1))$.

$(6,8,10)$ satisfies $6^2 + 8^2 = 10^2$ but it is not primitive since 2 divides $6, 8$, and 10.

Counting Pythagorean triples

$$F = x^2 + y^2 - z^2$$

$N(F, h)$: the number of primitive Pythagorean triples (x, y, z) with $|z|^2 \leqslant h$.

Theorem (Lehmer 1900, Lambek–Moser 1950)

$$\lim_{h \to \infty} \frac{N(F, h)}{h^{1/2}} = \frac{8}{\pi}.$$

Counting Pythagorean triples

$F = x^2 + y^2 - z^2$

$N(F, h)$: the number of primitive Pythagorean triples (x, y, z) with $|z|^2 \leqslant h$.

Theorem (Lehmer 1900, Lambek–Moser 1950)

$$\lim_{h\to\infty} \frac{N(F,h)}{h^{1/2}} = \frac{8}{\pi}.$$

Counting Pythagorean triples

$F = x^2 + y^2 - z^2$

$N(F, h)$: the number of primitive Pythagorean triples (x, y, z) with $|z|^2 \leqslant h$.

Theorem (Lehmer 1900, Lambek–Moser 1950)

$$\lim_{h \to \infty} \frac{N(F, h)}{h^{1/2}} = \frac{8}{\pi}.$$

Euler's theorem ($\chi = 0$)

$F = x^3 + y^3 - z^3$ defines an elliptic curve C with Mordell–Weil group $C(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

```
1
2   // Proof of Euler's theorem in Magma.
3
4   R<x,y,z> := PolynomialRing(Rationals(),3);
5   F := x^3 + y^3 - z^3;
6   P2 := ProjectiveSpace(R);
7   C := Curve(P2,F);
8   RationalPoints(C : Bound:=1000);
9   // {@ (0 : 1 : 1), (1 : 0 : 1), (-1 : 1 : 0) @}
10  Genus(C);
11  // Equals 1
12  C := EllipticCurve(C);
13  MordellWeilGroup(C);
14  // Equals Z/3Z
15
```

Euler's theorem ($\chi = 0$)

$F = x^3 + y^3 - z^3$ defines an elliptic curve C with Mordell–Weil group $C(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

```
1
2   // Proof of Euler's theorem in Magma.
3
4   R<x,y,z> := PolynomialRing(Rationals(),3);
5   F := x^3 + y^3 - z^3;
6   P2 := ProjectiveSpace(R);
7   C := Curve(P2,F);
8   RationalPoints(C : Bound:=1000);
9   // {@ (0 : 1 : 1), (1 : 0 : 1), (-1 : 1 : 0) @}
10  Genus(C);
11  // Equals 1
12  C := EllipticCurve(C);
13  MordellWeilGroup(C);
14  // Equals Z/3Z
15
```

Euler's theorem ($\chi = 0$)

$F = x^3 + y^3 - z^3$ defines an elliptic curve C with Mordell–Weil group $C(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

```
1
2     // Proof of Euler's theorem in Magma.
3
4     R<x,y,z> := PolynomialRing(Rationals(),3);
5     F := x^3 + y^3 - z^3;
6     P2 := ProjectiveSpace(R);
7     C := Curve(P2,F);
8     RationalPoints(C : Bound:=1000);
9     // {@ (0 : 1 : 1), (1 : 0 : 1), (-1 : 1 : 0) @}
10    Genus(C);
11    // Equals 1
12    C := EllipticCurve(C);
13    MordellWeilGroup(C);
14    // Equals Z/3Z
15
```

Faltings, Wiles, Taylor–Wiles ($\chi < 0$)

When $n > 3$, the equation $F = x^n + y^n - z^n$ defines a nice plane curve $C_n/\mathbb{Q}$ of genus $g > 1$.

Theorem (Faltings '83)

For each $n > 3$, the curve $C_n : x^n + y^n = z^n$ has finitely many rational points.

Theorem (Wiles '93, Taylor–Wiles '95)

The curves $C_n : x^n + y^n = z^n$ have at most four rational points. They all satisfy $x \cdot y \cdot z = 0$.

Faltings, Wiles, Taylor–Wiles ($\chi < 0$)

When $n > 3$, the equation $F = x^n + y^n - z^n$ defines a nice plane curve $C_n/\mathbb{Q}$ of genus $g > 1$.

Theorem (Faltings '83)

For each $n > 3$, the curve $C_n : x^n + y^n = z^n$ has finitely many rational points.

Theorem (Wiles '93, Taylor–Wiles '95)

The curves $C_n : x^n + y^n = z^n$ have at most four rational points. They all satisfy $x \cdot y \cdot z = 0$.

Faltings, Wiles, Taylor–Wiles ($\chi < 0$)

When $n > 3$, the equation $F = x^n + y^n - z^n$ defines a nice plane curve $C_n/\mathbb{Q}$ of genus $g > 1$.

Theorem (Faltings '83)

For each $n > 3$, the curve $C_n : x^n + y^n = z^n$ has finitely many rational points.

Theorem (Wiles '93, Taylor–Wiles '95)

The curves $C_n : x^n + y^n = z^n$ have at most four rational points. They all satisfy $x \cdot y \cdot z = 0$.

Generalized Fermat equations

$$F = Ax^a + By^b + Cz^c$$

A triple $(x, y, z) \in \mathbb{Z}$ is a primitive solution if $F(x, y, z) = 0$ and there is no prime p dividing x, y, and z

$$\chi := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$$

Generalized Fermat equations

$$F = Ax^a + By^b + Cz^c$$

A triple $(x, y, z) \in \mathbb{Z}$ is a primitive solution if $F(x, y, z) = 0$ and there is no prime p dividing x, y, and z

$$\chi := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$$

Generalized Fermat equations

$F = Ax^a + By^b + Cz^c$

A triple $(x, y, z) \in \mathbb{Z}$ is a primitive solution if $F(x, y, z) = 0$ and there is no prime p dividing x, y, and z

$\chi := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$

Spherical signatures

Let $F = Ax^a + By^b + Cz^c$ be a generalized Fermat equation with integer coefficients satisfying

$$\chi = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 > 0.$$

(a, b, c)	$\chi(a, b, c)$
$(2, 2, c)$	$1/c$
$(2, 3, 3)$	$1/6$
$(2, 3, 4)$	$1/12$
$(2, 3, 5)$	$1/30$

Spherical signatures

Let $F = Ax^a + By^b + Cz^c$ be a generalized Fermat equation with integer coefficients satisfying

$$\chi = \tfrac{1}{a} + \tfrac{1}{b} + \tfrac{1}{c} - 1 > 0.$$

(a, b, c)	$\chi(a, b, c)$
$(2, 2, c)$	$1/c$
$(2, 3, 3)$	$1/6$
$(2, 3, 4)$	$1/12$
$(2, 3, 5)$	$1/30$

Generalized "Pythagorean" triples

Theorem (Beukers '98)

There exist parametrizations for the primitive integral solutions to the spherical Fermat equations $Ax^a + By^b + Cz^c = 0$.

Example

For $(a, b, c) = (2, 2, 2)$, one of these parametric solutions is

$$x_1(s,t) = s^2 - t^2, \quad y_1(s,t) = 2st, \quad z_1(s,t) = s^2 + t^2.$$

Theorem (Edwards '04)

Complete parametrizations for the primitive integral solutions to the spherical equations $x^a + y^b = z^c$.

Example

When $(a, b, c) = (2, 3, 5)$, Edwards finds that there are 49 parametric solutions $\phi_\tau = (x_\tau(s,t), y_\tau(s,t), z_\tau(s,t))$ needed.

Generalized "Pythagorean" triples

Theorem (Beukers '98)

There exist parametrizations for the primitive integral solutions to the spherical Fermat equations $Ax^a + By^b + Cz^c = 0$.

Example

For $(a, b, c) = (2, 2, 2)$, one of these parametric solutions is

$$x_1(s, t) = s^2 - t^2, \quad y_1(s, t) = 2st, \quad z_1(s, t) = s^2 + t^2.$$

Theorem (Edwards '04)

Complete parametrizations for the primitive integral solutions to the spherical equations $x^a + y^b = z^c$.

Example

When $(a, b, c) = (2, 3, 5)$, Edwards finds that there are 49 parametric solutions $\phi_\tau = (x_\tau(s, t), y_\tau(s, t), z_\tau(s, t))$ needed.

Generalized "Pythagorean" triples

Theorem (Beukers '98)

There exist parametrizations for the primitive integral solutions to the spherical Fermat equations $Ax^a + By^b + Cz^c = 0$.

Example

For $(a, b, c) = (2, 2, 2)$, one of these parametric solutions is

$$x_1(s,t) = s^2 - t^2, \quad y_1(s,t) = 2st, \quad z_1(s,t) = s^2 + t^2.$$

Theorem (Edwards '04)

Complete parametrizations for the primitive integral solutions to the spherical equations $x^a + y^b = z^c$.

Example

When $(a, b, c) = (2, 3, 5)$, Edwards finds that there are 49 parametric solutions $\phi_\tau = (x_\tau(s,t), y_\tau(s,t), z_\tau(s,t))$ needed.

Generalized "Pythagorean" triples

Theorem (Beukers '98)

There exist parametrizations for the primitive integral solutions to the spherical Fermat equations $Ax^a + By^b + Cz^c = 0$.

Example

For $(a, b, c) = (2, 2, 2)$, one of these parametric solutions is

$$x_1(s,t) = s^2 - t^2, \quad y_1(s,t) = 2st, \quad z_1(s,t) = s^2 + t^2.$$

Theorem (Edwards '04)

Complete parametrizations for the primitive integral solutions to the spherical equations $x^a + y^b = z^c$.

Example

When $(a, b, c) = (2, 3, 5)$, Edwards finds that there are 49 parametric solutions $\phi_\tau = (x_\tau(s,t), y_\tau(s,t), z_\tau(s,t))$ needed.

Generalized "Pythagorean" triples

Theorem (Beukers '98)

There exist parametrizations for the primitive integral solutions to the spherical Fermat equations $Ax^a + By^b + Cz^c = 0$.

Example

For $(a, b, c) = (2, 2, 2)$, one of these parametric solutions is

$$x_1(s,t) = s^2 - t^2, \quad y_1(s,t) = 2st, \quad z_1(s,t) = s^2 + t^2.$$

Theorem (Edwards '04)

Complete parametrizations for the primitive integral solutions to the spherical equations $x^a + y^b = z^c$.

Example

When $(a, b, c) = (2, 3, 5)$, Edwards finds that there are 49 parametric solutions $\phi_\tau = (x_\tau(s,t), y_\tau(s,t), z_\tau(s,t))$ needed.

Generalized "Pythagorean" triples

Theorem (Beukers '98)

There exist parametrizations for the primitive integral solutions to the spherical Fermat equations $Ax^a + By^b + Cz^c = 0$.

Example

For $(a, b, c) = (2, 2, 2)$, one of these parametric solutions is

$$x_1(s,t) = s^2 - t^2, \quad y_1(s,t) = 2st, \quad z_1(s,t) = s^2 + t^2.$$

Theorem (Edwards '04)

Complete parametrizations for the primitive integral solutions to the spherical equations $x^a + y^b = z^c$.

Example

When $(a, b, c) = (2, 3, 5)$, Edwards finds that there are 49 parametric solutions $\phi_\tau = (x_\tau(s,t), y_\tau(s,t), z_\tau(s,t))$ needed.

Generalized Lehmer–Lambek–Moser

$F := Ax^a + By^b + Cz^c$

$\chi(F) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$

$N(F, h)$: the number of primitive integral solutions (x, y, z) to $F = 0$ with $\mathrm{Ht}_{\mathbb{P}^1}(Ax^a : Cz^c) \leqslant h$.

Theorem (A-P)

Suppose that $\chi > 0$ and $\mathcal{U}(\mathbb{Z}) \neq \emptyset$. Then, there exists an effectively computable constant $\kappa(F) > 0$ such that

$$\lim_{h \to \infty} \frac{N(F, h)}{h^{\chi}} = \kappa(F).$$

Generalized Lehmer–Lambek–Moser

$$F := Ax^a + By^b + Cz^c$$

$$\chi(F) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$$

$N(F, h)$: the number of primitive integral solutions (x, y, z) to $F = 0$ with $\mathrm{Ht}_{\mathbb{P}^1}(Ax^a : Cz^c) \leqslant h$.

Theorem (A-P)

Suppose that $\chi > 0$ and $\mathcal{U}(\mathbb{Z}) \neq \emptyset$. Then, there exists an effectively computable constant $\kappa(F) > 0$ such that

$$\lim_{h \to \infty} \frac{N(F, h)}{h^{\chi}} = \kappa(F).$$

Generalized Lehmer–Lambek–Moser

$$F := Ax^a + By^b + Cz^c$$

$$\chi(F) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$$

$N(F, h)$: the number of primitive integral solutions (x, y, z) to $F = 0$ with $\mathrm{Ht}_{\mathbb{P}^1}(Ax^a : Cz^c) \leqslant h$.

Theorem (A-P)

Suppose that $\chi > 0$ and $\mathcal{U}(\mathbb{Z}) \neq \emptyset$. Then, there exists an effectively computable constant $\kappa(F) > 0$ such that

$$\lim_{h \to \infty} \frac{N(F, h)}{h^{\chi}} = \kappa(F).$$

Generalized Lehmer–Lambek–Moser

$F := Ax^a + By^b + Cz^c$

$\chi(F) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$

$N(F, h)$: the number of primitive integral solutions (x, y, z) to $F = 0$ with $\mathrm{Ht}_{\mathbb{P}^1}(Ax^a : Cz^c) \leqslant h$.

Theorem (A-P)

Suppose that $\chi > 0$ and $\mathcal{U}(\mathbb{Z}) \neq \emptyset$. Then, there exists an effectively computable constant $\kappa(F) > 0$ such that

$$\lim_{h \to \infty} \frac{N(F, h)}{h^{\chi}} = \kappa(F).$$

Generalized Lehmer–Lambek–Moser

$F := Ax^a + By^b + Cz^c$

$\chi(F) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$

$N(F, h)$: the number of primitive integral solutions (x, y, z) to $F = 0$ with $\mathrm{Ht}_{\mathbb{P}^1}(Ax^a : Cz^c) \leqslant h$.

Theorem (A-P)

Suppose that $\chi > 0$ and $\mathcal{U}(\mathbb{Z}) \neq \emptyset$. Then, there exists an effectively computable constant $\kappa(F) > 0$ such that

$$\lim_{h \to \infty} \frac{N(F, h)}{h^{\chi}} = \kappa(F).$$

Generalized Faltings

Let $F = Ax^a + By^b + Cz^c$ be a generalized Fermat equation with integer coefficients satisfying

$$\chi = \tfrac{1}{a} + \tfrac{1}{b} + \tfrac{1}{c} - 1 < 0.$$

Theorem (Darmon–Granville '95)

The set of primitive integer solutions is finite.

Generalized Faltings

Let $F = Ax^a + By^b + Cz^c$ be a generalized Fermat equation with integer coefficients satisfying

$$\chi = \tfrac{1}{a} + \tfrac{1}{b} + \tfrac{1}{c} - 1 < 0.$$

Theorem (Darmon–Granville '95)

The set of primitive integer solutions is finite.

Generalized Faltings

Let $F = Ax^a + By^b + Cz^c$ be a generalized Fermat equation with integer coefficients satisfying

$$\chi = \tfrac{1}{a} + \tfrac{1}{b} + \tfrac{1}{c} - 1 < 0.$$

Theorem (Darmon–Granville '95)

The set of primitive integer solutions is finite.

Generalized Wiles: the million dollar question

Conjecture (Generalized Fermat conjecture - Beal's conjecture)

If $a, b, c \geqslant 3$, *the generalized Fermat equation* $F = x^a + y^b - z^c$ *has no nontrivial primitive solutions.*

Darmon's curves with multiplicities

Henri Darmon ('07):

> *Nonetheless, in this Diophantine study one is reluctant to abandon the well-tended landscape of curves for the untamed wilds of (singular) algebraic surfaces. As it turns out, a better framework for discussing primitive solutions of the generalized Fermat equation is supplied by the notion of a curve with multiplicities.*

Poonen–Schaefer–Stoll

PSS:

> *Keeping the stacks in the back of one's mind, however, still simplifies the task of finding the étale covers of the punctured surfaces; we will use them for this purpose.*

Theorem (PSS '07)

The primitive integer solutions to $x^2 + y^3 = z^7$ *are the 16 triples*

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

Poonen–Schaefer–Stoll

PSS:

> *Keeping the stacks in the back of one's mind, however, still simplifies the task of finding the étale covers of the punctured surfaces; we will use them for this purpose.*

Theorem (PSS '07)

The primitive integer solutions to $x^2 + y^3 = z^7$ *are the 16 triples*

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

Stacky curves

My thesis:

> *Nonetheless, in this Diophantine study one is reluctant to abandon the well-tended landscape of curves for the untamed wilds of (singular) algebraic surfaces. As it turns out, a better framework for discussing primitive solutions of the generalized Fermat equation is supplied by the notion of a ~~curve with multiplicities~~ stacky curve.*

Torsors

S a base scheme

$G \to S$ an fppf group scheme

Definition (Torsor scheme)

A right fppf G-torsor over S is an S-scheme $T \to S$ together with a right action $T \times_S G \to T$ such that the following conditions hold:

1. $T \to S$ is fppf.
2. The map $T \times_S G \to T \times_S T$ defined by $(t, g) \mapsto (t, t \cdot g)$ is an isomorphism.

A morphism of G-torsors is a G-equivariant morphism of S-schemes.

Torsors

S a base scheme

$G \to S$ an fppf group scheme

Definition (Torsor scheme)

A right fppf G-torsor over S is an S-scheme $T \to S$ together with a right action $T \times_S G \to T$ such that the following conditions hold:

1. $T \to S$ is fppf.
2. The map $T \times_S G \to T \times_S T$ defined by $(t, g) \mapsto (t, t \cdot g)$ is an isomorphism.

A morphism of G-torsors is a G-equivariant morphism of S-schemes.

Torsors

S a base scheme

$G \to S$ an fppf group scheme

Definition (Torsor scheme)

A right fppf G-torsor over S is an S-scheme $T \to S$ together with a right action $T \times_S G \to T$ such that the following conditions hold:

1. $T \to S$ is fppf.
2. The map $T \times_S G \to T \times_S T$ defined by $(t, g) \mapsto (t, t \cdot g)$ is an isomorphism.

A morphism of G-torsors is a G-equivariant morphism of S-schemes.

Torsors

S a base scheme

$G \to S$ an fppf group scheme

Definition (Torsor scheme)

A right fppf G-torsor over S is an S-scheme $T \to S$ together with a right action $T \times_S G \to T$ such that the following conditions hold:

1. $T \to S$ is fppf.
2. The map $T \times_S G \to T \times_S T$ defined by $(t, g) \mapsto (t, t \cdot g)$ is an isomorphism.

A morphism of G-torsors is a G-equivariant morphism of S-schemes.

Torsors

S a base scheme

$G \to S$ an fppf group scheme

Definition (Torsor scheme)

A right fppf G-torsor over S is an S-scheme $T \to S$ together with a right action $T \times_S G \to T$ such that the following conditions hold:

1. $T \to S$ is fppf.
2. The map $T \times_S G \to T \times_S T$ defined by $(t, g) \mapsto (t, t \cdot g)$ is an isomorphism.

A morphism of G-torsors is a G-equivariant morphism of S-schemes.

H^1

S a locally noetherian scheme

$G \to S$ an fppf group scheme

Theorem

Suppose that one of the following conditions holds:

(i) *$G \to S$ is affine.*

(ii) *G is of finite presentation, separated over S, and* $\dim S \leqslant 1$.

(iii) *$G \to S$ is an abelian scheme, and G is locally factorial.*

Then, we have a bijection of pointed sets

$$\frac{\{G\text{-torsor schemes}\}}{\cong} \xrightarrow{\sim} \check{\mathrm{H}}^1_{fppf}(S, G).$$

$\mathrm{H}^1(S, G) := \check{\mathrm{H}}^1_{\mathtt{fppf}}(S, G)$.

H^1

S a locally noetherian scheme

$G \to S$ an fppf group scheme

Theorem

Suppose that one of the following conditions holds:

(i) *$G \to S$ is affine.*

(ii) *G is of finite presentation, separated over S, and $\dim S \leqslant 1$.*

(iii) *$G \to S$ is an abelian scheme, and G is locally factorial.*

Then, we have a bijection of pointed sets

$$\frac{\{G\text{-torsor schemes}\}}{\cong} \xrightarrow{\sim} \check{\mathrm{H}}^1_{fppf}(S, G).$$

$$\mathrm{H}^1(S, G) := \check{\mathrm{H}}^1_{\mathtt{fppf}}(S, G).$$

H^1

S a locally noetherian scheme

$G \to S$ an fppf group scheme

Theorem

Suppose that one of the following conditions holds:

(i) *$G \to S$ is affine.*

(ii) *G is of finite presentation, separated over S, and $\dim S \leqslant 1$.*

(iii) *$G \to S$ is an abelian scheme, and G is locally factorial.*

Then, we have a bijection of pointed sets

$$\frac{\{G\text{-torsor schemes}\}}{\cong} \xrightarrow{\sim} \check{\mathrm{H}}^1_{fppf}(S, G).$$

$$\mathrm{H}^1(S, G) := \check{\mathrm{H}}^1_{\mathrm{fppf}}(S, G).$$

H^1

S a locally noetherian scheme

$G \to S$ an fppf group scheme

Theorem

Suppose that one of the following conditions holds:

(i) *$G \to S$ is affine.*

(ii) *G is of finite presentation, separated over S, and* $\dim S \leqslant 1$.

(iii) *$G \to S$ is an abelian scheme, and G is locally factorial.*

Then, we have a bijection of pointed sets

$$\frac{\{G\text{-torsor schemes}\}}{\cong} \xrightarrow{\sim} \check{\mathrm{H}}^1_{fppf}(S, G).$$

$$\mathrm{H}^1(S, G) := \check{\mathrm{H}}^1_{\mathtt{fppf}}(S, G).$$

Quotient stacks

S a scheme
G an fppf group scheme over S
Z a scheme over S, with a right G action
We obtain the quotient stack $[Z/G]$

For a test scheme $U \in \mathtt{Sch}_S$, we get a groupoid $[Z/G](U)$ whose objects are triples (U, T, ϕ):

Example

If Z is a G-torsor, then $[Z/G] \cong S$.

Quotient stacks

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

We obtain the quotient stack $[Z/G]$

For a test scheme $U \in \mathtt{Sch}_S$, we get a groupoid $[Z/G](U)$ whose objects are triples (U, T, ϕ):

Example

If Z is a G-torsor, then $[Z/G] \cong S$.

Quotient stacks

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

We obtain the quotient stack $[Z/G]$

For a test scheme $U \in \mathtt{Sch}_S$, we get a groupoid $[Z/G](U)$ whose objects are triples (U, T, ϕ):

Example

If Z is a G-torsor, then $[Z/G] \cong S$.

Quotient stacks

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

We obtain the quotient stack $[Z/G]$

For a test scheme $U \in \mathtt{Sch}_S$, we get a groupoid $[Z/G](U)$ whose objects are triples (U, T, ϕ):

Example

If Z is a G-torsor, then $[Z/G] \cong S$.

Quotient stacks

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

We obtain the quotient stack $[Z/G]$

For a test scheme $U \in \mathtt{Sch}_S$, we get a groupoid $[Z/G](U)$ whose objects are triples (U, T, ϕ):

Example

If Z is a G-torsor, then $[Z/G] \cong S$.

Quotient stacks

S a scheme
G an fppf group scheme over S
Z a scheme over S, with a right G action
We obtain the quotient stack $[Z/G]$

For a test scheme $U \in \mathtt{Sch}_S$, we get a groupoid $[Z/G](U)$ whose objects are triples (U, T, ϕ):

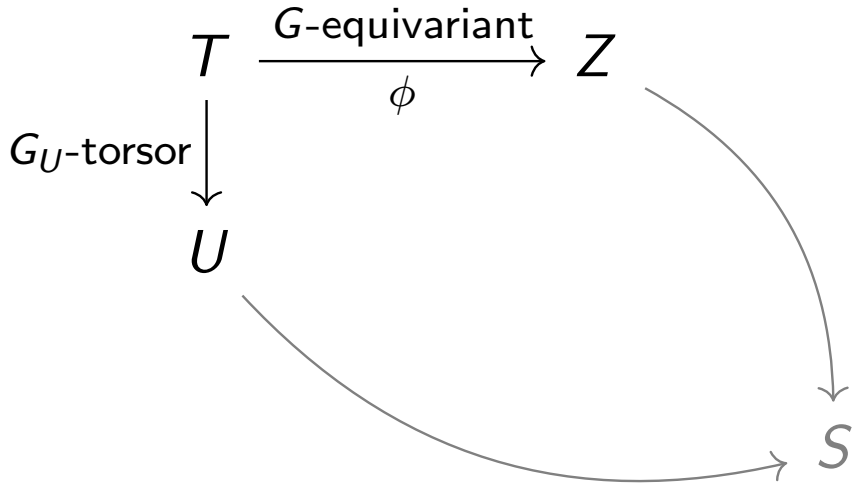
Example

If Z is a G-torsor, then $[Z/G] \cong S$.

Quotient stacks

S a scheme
G an fppf group scheme over S
Z a scheme over S, with a right G action
We obtain the quotient stack $[Z/G]$

For a test scheme $U \in \mathtt{Sch}_S$, we get a groupoid $[Z/G](U)$ whose objects are triples (U, T, ϕ):



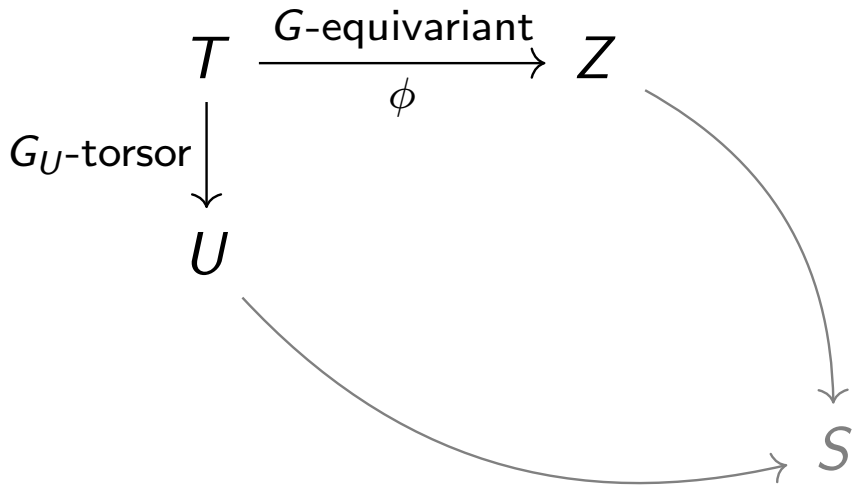
Example

If Z is a G-torsor, then $[Z/G] \cong S$.

Quotient stacks

S a scheme
G an fppf group scheme over S
Z a scheme over S, with a right G action
We obtain the quotient stack $[Z/G]$

For a test scheme $U \in \mathtt{Sch}_S$, we get a groupoid $[Z/G](U)$ whose objects are triples (U, T, ϕ):



Example

If Z is a G-torsor, then $[Z/G] \cong S$.

Twisting by fppf descent

We have the natural map $f : Z \to [Z/G]$ sending $z \in Z(U)$ to the diagram

If $T \to S$ is a **left** G-torsor corresponding to $\tau \in \mathrm{H}^1(S, G)$, we have a twist $f^\tau : Z^\tau \to [Z/G]$.

Z^τ is defined to be the contracted product $[Z \overset{G}{\times} T/G]$.

Twisting by fppf descent

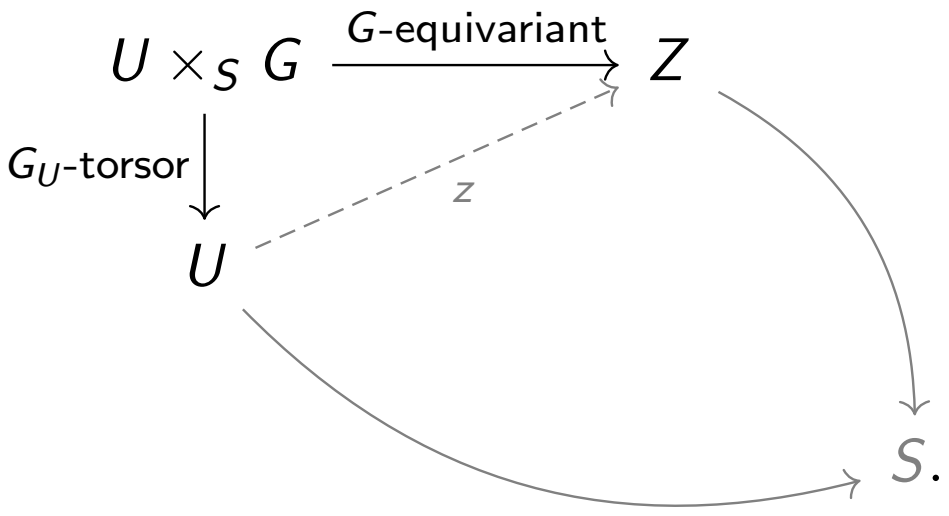
We have the natural map $f : Z \to [Z/G]$ sending $z \in Z(U)$ to the diagram

If $T \to S$ is a **left** G-torsor corresponding to $\tau \in \mathrm{H}^1(S, G)$, we have a twist $f^\tau : Z^\tau \to [Z/G]$.

Z^τ is defined to be the contracted product $[Z \overset{G}{\times} T/G]$.

Twisting by fppf descent

We have the natural map $f : Z \to [Z/G]$ sending $z \in Z(U)$ to the diagram

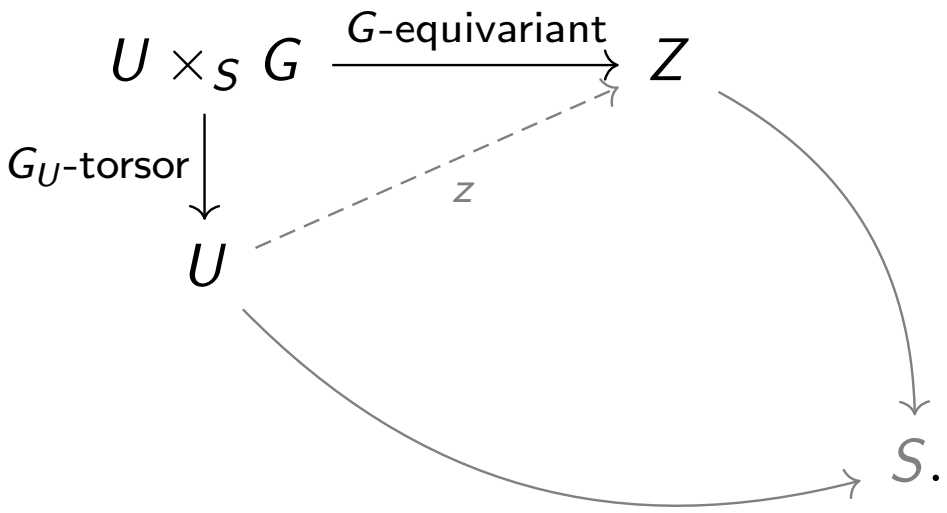


If $T \to S$ is a **left** G-torsor corresponding to $\tau \in \mathrm{H}^1(S, G)$, we have a twist $f^\tau : Z^\tau \to [Z/G]$.

Z^τ is defined to be the contracted product $[Z \overset{G}{\times} T/G]$.

Twisting by fppf descent

We have the natural map $f : Z \to [Z/G]$ sending $z \in Z(U)$ to the diagram



If $T \to S$ is a **left** G-torsor corresponding to $\tau \in \mathrm{H}^1(S, G)$, we have a twist $f^\tau : Z^\tau \to [Z/G]$.

Z^τ is defined to be the contracted product $[Z \overset{G}{\times} T/G]$.

The method of descent

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

If $\mathscr{X}$ is a stack, $\mathscr{X}\langle S\rangle$ is the set of isomorphism classes in $\mathscr{X}(S)$

Theorem

$$[Z/G]\langle S\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(S,G)} f^\tau(Z^\tau(S)).$$

Proof:

□

The method of descent

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

If $\mathscr{X}$ is a stack, $\mathscr{X}\langle S\rangle$ is the set of isomorphism classes in $\mathscr{X}(S)$

Theorem

$$[Z/G]\langle S\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(S,G)} f^\tau(Z^\tau(S)).$$

Proof:

$$\begin{array}{ccccc}
 & & T^{-1}\overset{G}{\times}T & \xrightarrow{\phi\times \mathrm{id}_T} & Z^\tau \\
 & \overset{e}{\nearrow} & \downarrow & & \downarrow f^\tau \\
S & \longrightarrow & T^{-1} & \xrightarrow{\phi} & Z \\
 & & \downarrow & & \downarrow f \\
 & & S & \longrightarrow & [Z/G] \\
 & & & & \| \\
 & & & & [Z/G]
\end{array}$$

□

The method of descent

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

If $\mathscr{X}$ is a stack, $\mathscr{X}\langle S\rangle$ is the set of isomorphism classes in $\mathscr{X}(S)$

Theorem

$$[Z/G]\langle S\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(S,G)} f^\tau(Z^\tau(S)).$$

Proof:

$$\begin{array}{ccccc}
T^{-1}\overset{G}{\times}T & & \xrightarrow{\phi\times \mathrm{id}_T} & & Z^\tau \\
\uparrow e & & & & \\
T^{-1} & \xrightarrow{\phi} & Z & & \downarrow f^\tau \\
\downarrow & & \downarrow f & & \\
S & \longrightarrow & [Z/G] & = & [Z/G]
\end{array}$$

□

The method of descent

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

If $\mathscr{X}$ is a stack, $\mathscr{X}\langle S\rangle$ is the set of isomorphism classes in $\mathscr{X}(S)$

Theorem

$$[Z/G]\langle S\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(S,G)} f^\tau(Z^\tau(S)).$$

Proof:

$$\begin{array}{ccccc}
 & & {}^{G}T^{-1}\times T & \xrightarrow{\phi\times \mathrm{id}_T} & Z^\tau \\
 & \overset{e}{\nearrow} & \downarrow & & \downarrow f^\tau \\
S & \longrightarrow & [Z/G] & = & [Z/G]
\end{array}$$

$$\begin{array}{ccc}
T^{-1} & \xrightarrow{\phi} & Z \\
\downarrow & & \downarrow f \\
S & \longrightarrow & [Z/G]
\end{array}$$

□

The method of descent

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

If $\mathscr{X}$ is a stack, $\mathscr{X}\langle S\rangle$ is the set of isomorphism classes in $\mathscr{X}(S)$

Theorem

$$[Z/G]\langle S\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(S,G)} f^\tau(Z^\tau(S)).$$

Proof:

$$\begin{array}{ccccc}
 & & {}^{G}T^{-1}\times T & \xrightarrow{\phi\times \mathrm{id}_T} & Z^\tau \\
 & \overset{e}{\nearrow} & \downarrow & & \downarrow f^\tau \\
S & \longrightarrow & [Z/G] & = & [Z/G]
\end{array}$$

$$\begin{array}{ccc}
T^{-1} & \xrightarrow{\phi} & Z \\
\downarrow & & \downarrow f \\
S & \longrightarrow & [Z/G]
\end{array}$$

□

The method of descent

S a scheme

G an fppf group scheme over S

Z a scheme over S, with a right G action

If $\mathscr{X}$ is a stack, $\mathscr{X}\langle S\rangle$ is the set of isomorphism classes in $\mathscr{X}(S)$

Theorem

$$[Z/G]\langle S\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(S,G)} f^\tau(Z^\tau(S)).$$

Proof:

□

The method of descent

S a scheme

G an fppf group scheme over S

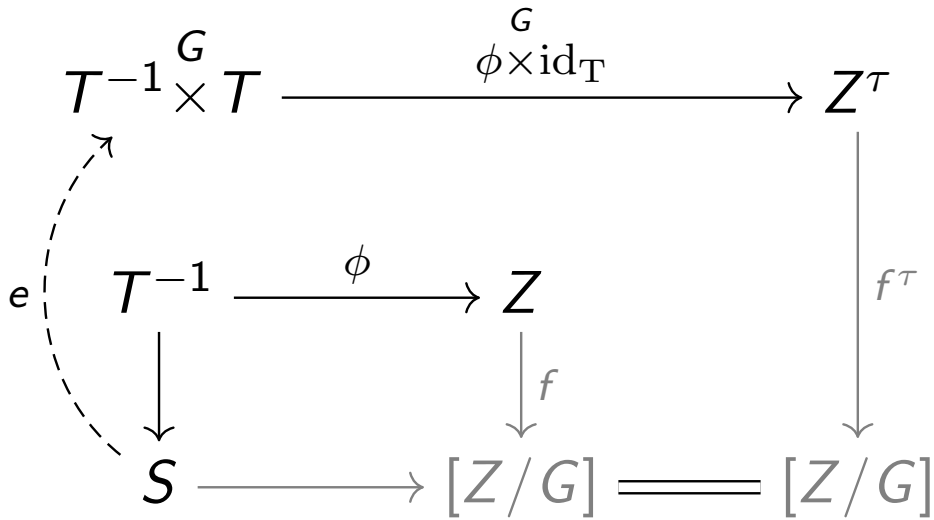
Z a scheme over S, with a right G action

If $\mathscr{X}$ is a stack, $\mathscr{X}\langle S\rangle$ is the set of isomorphism classes in $\mathscr{X}(S)$

Theorem

$$[Z/G]\langle S\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(S,G)} f^\tau(Z^\tau(S)).$$

Proof:



□

Pythagorean triples (via the method of descent)

$$\phi(s,t) := (s^2 - t^2, 2st, s^2 + t^2), \quad \hat{\phi}(s,t) := (2st, s^2 - t^2, s^2 + t^2).$$

Theorem (300 BC)

Every primitive integral solution (x, y, z) *to the Diophantine equation* $x^2 + y^2 = z^2$ *corresponds to*

$$\phi(s,t), \quad -\phi(s,t), \quad \hat{\phi}(s,t), \quad -\hat{\phi}(s,t),$$

for a unique pair of tuples $\pm(s,t) \in \mathbb{Z}^2$ *satisfying* $\gcd(s,t) = 1$ *and* $s \not\equiv t \mod 2$.

Proof: Covering, twisting, sieving. □

Pythagorean triples (via the method of descent)

$$\phi(s,t) := (s^2 - t^2, 2st, s^2 + t^2), \quad \hat{\phi}(s,t) := (2st, s^2 - t^2, s^2 + t^2).$$

Theorem (300 BC)

Every primitive integral solution (x, y, z) *to the Diophantine equation* $x^2 + y^2 = z^2$ *corresponds to*

$$\phi(s,t), \quad -\phi(s,t), \quad \hat{\phi}(s,t), \quad -\hat{\phi}(s,t),$$

for a unique pair of tuples $\pm(s,t) \in \mathbb{Z}^2$ *satisfying* $\gcd(s,t) = 1$ *and* $s \not\equiv t \mod 2$.

Proof: Covering, twisting, sieving. $\square$

Step 1: covering

$\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$ over $\mathbb{Z}$

$\mathcal{V}(\mathbb{Z}) = \{(s,t) \in \mathbb{Z}^2 : \gcd(s,t) = 1\}$

$\mathcal{U} := \operatorname{Spec} \mathbb{Z}[x,y,z]/\langle x^2 + y^2 - z^2 \rangle - \mathbf{0}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive Pythagorean triples

$R := \mathbb{Z}[1/2]$ will be our base

$\mu_2 := \operatorname{Spec} R[u]/\langle u^2 - 1 \rangle$ acts on $\mathcal{V}_R$ via $(s,t) \cdot \zeta = (\zeta s, \zeta t)$.

Lemma

The map $\phi\colon \mathcal{V}_R \to \mathcal{U}_R$ given by $(s,t) \mapsto (s^2 - t^2, 2st, s^2 + t^2)$ is a μ_2-torsor. In particular, $[\mathcal{V}_R/\mu_2] = \mathcal{U}_R$.

Proof idea: $R[x,y,z]/\langle F \rangle \cong R[s^2 - t^2, 2st, s^2 + t^2]$ is the ring of invariants $R[s,t]^{\{\pm 1\}}$. (Note that this is not true over $\mathbb{Z}$!) $\square$

Step 1: covering

$\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$ over $\mathbb{Z}$

$\mathcal{V}(\mathbb{Z}) = \{(s,t) \in \mathbb{Z}^2 : \gcd(s,t) = 1\}$

$\mathcal{U} := \operatorname{Spec} \mathbb{Z}[x,y,z]/\langle x^2 + y^2 - z^2 \rangle - \mathbf{0}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive Pythagorean triples

$R := \mathbb{Z}[1/2]$ will be our base

$\mu_2 := \operatorname{Spec} R[u]/\langle u^2 - 1 \rangle$ acts on $\mathcal{V}_R$ via $(s,t) \cdot \zeta = (\zeta s, \zeta t)$.

Lemma

The map $\phi\colon \mathcal{V}_R \to \mathcal{U}_R$ given by $(s,t) \mapsto (s^2 - t^2, 2st, s^2 + t^2)$ is a μ_2-torsor. In particular, $[\mathcal{V}_R/\mu_2] = \mathcal{U}_R$.

Proof idea: $R[x,y,z]/\langle F \rangle \cong R[s^2 - t^2, 2st, s^2 + t^2]$ is the ring of invariants $R[s,t]^{\{\pm 1\}}$. (Note that this is not true over $\mathbb{Z}$!) $\square$

Step 1: covering

$\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$ over $\mathbb{Z}$

$\mathcal{V}(\mathbb{Z}) = \{(s,t) \in \mathbb{Z}^2 : \gcd(s,t) = 1\}$

$\mathcal{U} := \operatorname{Spec} \mathbb{Z}[x,y,z]/\langle x^2 + y^2 - z^2 \rangle - \mathbf{0}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive Pythagorean triples

$R := \mathbb{Z}[1/2]$ will be our base

$\mu_2 := \operatorname{Spec} R[u]/\langle u^2 - 1 \rangle$ acts on $\mathcal{V}_R$ via $(s,t) \cdot \zeta = (\zeta s, \zeta t)$.

Lemma

The map $\phi\colon \mathcal{V}_R \to \mathcal{U}_R$ given by $(s,t) \mapsto (s^2 - t^2, 2st, s^2 + t^2)$ is a μ_2-torsor. In particular, $[\mathcal{V}_R/\mu_2] = \mathcal{U}_R$.

Proof idea: $R[x,y,z]/\langle F \rangle \cong R[s^2 - t^2, 2st, s^2 + t^2]$ is the ring of invariants $R[s,t]^{\{\pm 1\}}$. (Note that this is not true over $\mathbb{Z}$!) $\square$

Step 1: covering

$\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$ over $\mathbb{Z}$

$\mathcal{V}(\mathbb{Z}) = \{(s,t) \in \mathbb{Z}^2 : \gcd(s,t) = 1\}$

$\mathcal{U} := \operatorname{Spec} \mathbb{Z}[x,y,z]/\langle x^2 + y^2 - z^2 \rangle - \mathbf{0}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive Pythagorean triples

$R := \mathbb{Z}[1/2]$ will be our base

$\mu_2 := \operatorname{Spec} R[u]/\langle u^2 - 1 \rangle$ acts on $\mathcal{V}_R$ via $(s,t) \cdot \zeta = (\zeta s, \zeta t)$.

Lemma

The map $\phi\colon \mathcal{V}_R \to \mathcal{U}_R$ given by $(s,t) \mapsto (s^2 - t^2, 2st, s^2 + t^2)$ is a μ_2-torsor. In particular, $[\mathcal{V}_R/\mu_2] = \mathcal{U}_R$.

Proof idea: $R[x,y,z]/\langle F \rangle \cong R[s^2 - t^2, 2st, s^2 + t^2]$ is the ring of invariants $R[s,t]^{\{\pm 1\}}$. (Note that this is not true over $\mathbb{Z}$!) $\square$

Step 1: covering

$\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$ over $\mathbb{Z}$

$\mathcal{V}(\mathbb{Z}) = \{(s,t) \in \mathbb{Z}^2 : \gcd(s,t) = 1\}$

$\mathcal{U} := \operatorname{Spec} \mathbb{Z}[x,y,z]/\langle x^2 + y^2 - z^2 \rangle - \mathbf{0}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive Pythagorean triples

$R := \mathbb{Z}[1/2]$ will be our base

$\mu_2 := \operatorname{Spec} R[u]/\langle u^2 - 1 \rangle$ acts on $\mathcal{V}_R$ via $(s,t) \cdot \zeta = (\zeta s, \zeta t)$.

Lemma

The map $\phi\colon \mathcal{V}_R \to \mathcal{U}_R$ given by $(s,t) \mapsto (s^2 - t^2, 2st, s^2 + t^2)$ is a μ_2-torsor. In particular, $[\mathcal{V}_R/\mu_2] = \mathcal{U}_R$.

Proof idea: $R[x,y,z]/\langle F \rangle \cong R[s^2 - t^2, 2st, s^2 + t^2]$ is the ring of invariants $R[s,t]^{\{\pm 1\}}$. (Note that this is not true over $\mathbb{Z}$!) $\square$

Step 1: covering

$\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$ over $\mathbb{Z}$

$\mathcal{V}(\mathbb{Z}) = \{(s,t) \in \mathbb{Z}^2 : \gcd(s,t) = 1\}$

$\mathcal{U} := \operatorname{Spec} \mathbb{Z}[x,y,z]/\langle x^2 + y^2 - z^2 \rangle - \mathbf{0}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive Pythagorean triples

$R := \mathbb{Z}[1/2]$ will be our base

$\mu_2 := \operatorname{Spec} R[u]/\langle u^2 - 1 \rangle$ acts on $\mathcal{V}_R$ via $(s,t) \cdot \zeta = (\zeta s, \zeta t)$.

Lemma

The map $\phi\colon \mathcal{V}_R \to \mathcal{U}_R$ given by $(s,t) \mapsto (s^2 - t^2, 2st, s^2 + t^2)$ is a μ_2-torsor. In particular, $[\mathcal{V}_R/\mu_2] = \mathcal{U}_R$.

Proof idea: $R[x,y,z]/\langle F \rangle \cong R[s^2 - t^2, 2st, s^2 + t^2]$ is the ring of invariants $R[s,t]^{\{\pm 1\}}$. (Note that this is not true over $\mathbb{Z}$!) $\square$

Step 1: covering

$\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$ over $\mathbb{Z}$

$\mathcal{V}(\mathbb{Z}) = \{(s,t) \in \mathbb{Z}^2 : \gcd(s,t) = 1\}$

$\mathcal{U} := \operatorname{Spec} \mathbb{Z}[x,y,z]/\langle x^2 + y^2 - z^2 \rangle - \mathbf{0}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive Pythagorean triples

$R := \mathbb{Z}[1/2]$ will be our base

$\mu_2 := \operatorname{Spec} R[u]/\langle u^2 - 1 \rangle$ acts on $\mathcal{V}_R$ via $(s,t) \cdot \zeta = (\zeta s, \zeta t)$.

Lemma

The map $\phi\colon \mathcal{V}_R \to \mathcal{U}_R$ given by $(s,t) \mapsto (s^2 - t^2, 2st, s^2 + t^2)$ is a μ_2-torsor. In particular, $[\mathcal{V}_R/\mu_2] = \mathcal{U}_R$.

Proof idea: $R[x,y,z]/\langle F \rangle \cong R[s^2 - t^2, 2st, s^2 + t^2]$ is the ring of invariants $R[s,t]^{\{\pm 1\}}$. (Note that this is not true over $\mathbb{Z}$!) $\square$

Step 1: covering

$\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$ over $\mathbb{Z}$

$\mathcal{V}(\mathbb{Z}) = \{(s,t) \in \mathbb{Z}^2 : \gcd(s,t) = 1\}$

$\mathcal{U} := \operatorname{Spec} \mathbb{Z}[x,y,z]/\langle x^2 + y^2 - z^2 \rangle - \mathbf{0}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive Pythagorean triples

$R := \mathbb{Z}[1/2]$ will be our base

$\mu_2 := \operatorname{Spec} R[u]/\langle u^2 - 1 \rangle$ acts on $\mathcal{V}_R$ via $(s,t) \cdot \zeta = (\zeta s, \zeta t)$.

Lemma

The map $\phi\colon \mathcal{V}_R \to \mathcal{U}_R$ given by $(s,t) \mapsto (s^2 - t^2, 2st, s^2 + t^2)$ is a μ_2-torsor. In particular, $[\mathcal{V}_R/\mu_2] = \mathcal{U}_R$.

Proof idea: $R[x,y,z]/\langle F \rangle \cong R[s^2 - t^2, 2st, s^2 + t^2]$ is the ring of invariants $R[s,t]^{\{\pm 1\}}$. (Note that this is not true over $\mathbb{Z}$!) $\square$

Step 2: twisting

By the method of descent, we have

$$\mathcal{U}(R) = [\mathcal{V}_R/\mu_2]\langle R\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(R,\mu_2)} \phi^\tau(\mathcal{V}^\tau(R)).$$

Lemma

$\mathrm{H}^1(R,\mu_2) \cong R^\times/(R^\times)^2 \cong \{\pm 1, \pm 2\}$. *For each* $d \in \{\pm 1, \pm 2\}$ *we have the torsor* $T_d := \operatorname{Spec} R[u]/\langle u^2 - d\rangle$.

Lemma

For each $d \in \{\pm 1, \pm 2\}$, *the twist of* ϕ *are* $\phi_d \colon \mathcal{V}_R \to \mathcal{U}_R$, *with* $\phi_d(s,t) := \frac{1}{d}\phi(s,t)$.

Summarizing,

$$\mathcal{U}(R) = \bigsqcup_{d\in\{\pm 1,\pm 2\}} \phi_d(\mathcal{V}(R)).$$

Step 2: twisting

By the method of descent, we have

$$\mathcal{U}(R) = [\mathcal{V}_R/\mu_2]\langle R\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(R,\mu_2)} \phi^\tau(\mathcal{V}^\tau(R)).$$

Lemma

$\mathrm{H}^1(R,\mu_2) \cong R^\times/(R^\times)^2 \cong \{\pm 1, \pm 2\}$. For each $d \in \{\pm 1, \pm 2\}$ we have the torsor $T_d := \operatorname{Spec} R[u]/\langle u^2 - d\rangle$.

Lemma

For each $d \in \{\pm 1, \pm 2\}$, the twist of ϕ are $\phi_d \colon \mathcal{V}_R \to \mathcal{U}_R$, with $\phi_d(s,t) := \frac{1}{d}\phi(s,t)$.

Summarizing,

$$\mathcal{U}(R) = \bigsqcup_{d\in\{\pm 1,\pm 2\}} \phi_d(\mathcal{V}(R)).$$

Step 2: twisting

By the method of descent, we have

$$\mathcal{U}(R) = [\mathcal{V}_R/\mu_2]\langle R\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(R,\mu_2)} \phi^\tau(\mathcal{V}^\tau(R)).$$

Lemma

$\mathrm{H}^1(R,\mu_2) \cong R^\times/(R^\times)^2 \cong \{\pm 1, \pm 2\}$. *For each* $d \in \{\pm 1, \pm 2\}$ *we have the torsor* $T_d := \operatorname{Spec} R[u]/\langle u^2 - d\rangle$.

Lemma

For each $d \in \{\pm 1, \pm 2\}$, *the twist of* ϕ *are* $\phi_d \colon \mathcal{V}_R \to \mathcal{U}_R$, *with* $\phi_d(s,t) := \frac{1}{d}\phi(s,t)$.

Summarizing,

$$\mathcal{U}(R) = \bigsqcup_{d\in\{\pm 1,\pm 2\}} \phi_d(\mathcal{V}(R)).$$

Step 2: twisting

By the method of descent, we have

$$\mathcal{U}(R) = [\mathcal{V}_R/\mu_2]\langle R\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(R,\mu_2)} \phi^\tau(\mathcal{V}^\tau(R)).$$

Lemma

$\mathrm{H}^1(R,\mu_2) \cong R^\times/(R^\times)^2 \cong \{\pm 1, \pm 2\}$. *For each* $d \in \{\pm 1, \pm 2\}$ *we have the torsor* $T_d := \operatorname{Spec} R[u]/\langle u^2 - d\rangle$.

Lemma

For each $d \in \{\pm 1, \pm 2\}$, *the twist of* ϕ *are* $\phi_d \colon \mathcal{V}_R \to \mathcal{U}_R$, *with* $\phi_d(s,t) := \frac{1}{d}\phi(s,t)$.

Summarizing,

$$\mathcal{U}(R) = \bigsqcup_{d\in\{\pm 1,\pm 2\}} \phi_d(\mathcal{V}(R)).$$

Step 2: twisting

By the method of descent, we have

$$\mathcal{U}(R) = [\mathcal{V}_R/\mu_2]\langle R\rangle = \bigsqcup_{\tau\in \mathrm{H}^1(R,\mu_2)} \phi^\tau(\mathcal{V}^\tau(R)).$$

Lemma

$\mathrm{H}^1(R,\mu_2) \cong R^\times/(R^\times)^2 \cong \{\pm 1, \pm 2\}$. *For each* $d \in \{\pm 1, \pm 2\}$ *we have the torsor* $T_d := \operatorname{Spec} R[u]/\langle u^2 - d\rangle$.

Lemma

For each $d \in \{\pm 1, \pm 2\}$, *the twist of* ϕ *are* $\phi_d \colon \mathcal{V}_R \to \mathcal{U}_R$, *with* $\phi_d(s,t) := \frac{1}{d}\phi(s,t)$.

Summarizing,

$$\mathcal{U}(R) = \bigsqcup_{d\in\{\pm 1,\pm 2\}} \phi_d(\mathcal{V}(R)).$$

Step 3: sieving

Goal: understand $\mathcal{U}(\mathbb{Z}) \cap \phi_d(\mathcal{V}(R))$.

Lemma

For each $d \in \{\pm 1, \pm 2\}$, we have that

$$\mathcal{U}(\mathbb{Z}) \cap \phi_d(\mathcal{V}(R)) = \phi_d(\mathcal{V}(\mathbb{Z})_{|d|}) = \begin{cases} \phi(\mathcal{V}(\mathbb{Z})_1), & \text{if } d = 1, \\ -\phi(\mathcal{V}(\mathbb{Z})_1), & \text{if } d = -1, \\ \hat{\phi}(\mathcal{V}(\mathbb{Z})_1), & \text{if } d = 2, \\ -\hat{\phi}(\mathcal{V}(\mathbb{Z})_1), & \text{if } d = -2. \end{cases}$$

Step 3: sieving

Goal: understand $\mathcal{U}(\mathbb{Z}) \cap \phi_d(\mathcal{V}(R))$.

Lemma

For each $d \in \{\pm 1, \pm 2\}$, we have that

$$\mathcal{U}(\mathbb{Z}) \cap \phi_d(\mathcal{V}(R)) = \phi_d(\mathcal{V}(\mathbb{Z})_{|d|}) = \begin{cases} \phi(\mathcal{V}(\mathbb{Z})_1), & \text{if } d = 1, \\ -\phi(\mathcal{V}(\mathbb{Z})_1), & \text{if } d = -1, \\ \hat{\phi}(\mathcal{V}(\mathbb{Z})_1), & \text{if } d = 2, \\ -\hat{\phi}(\mathcal{V}(\mathbb{Z})_1), & \text{if } d = -2. \end{cases}$$

Step 3: sieving

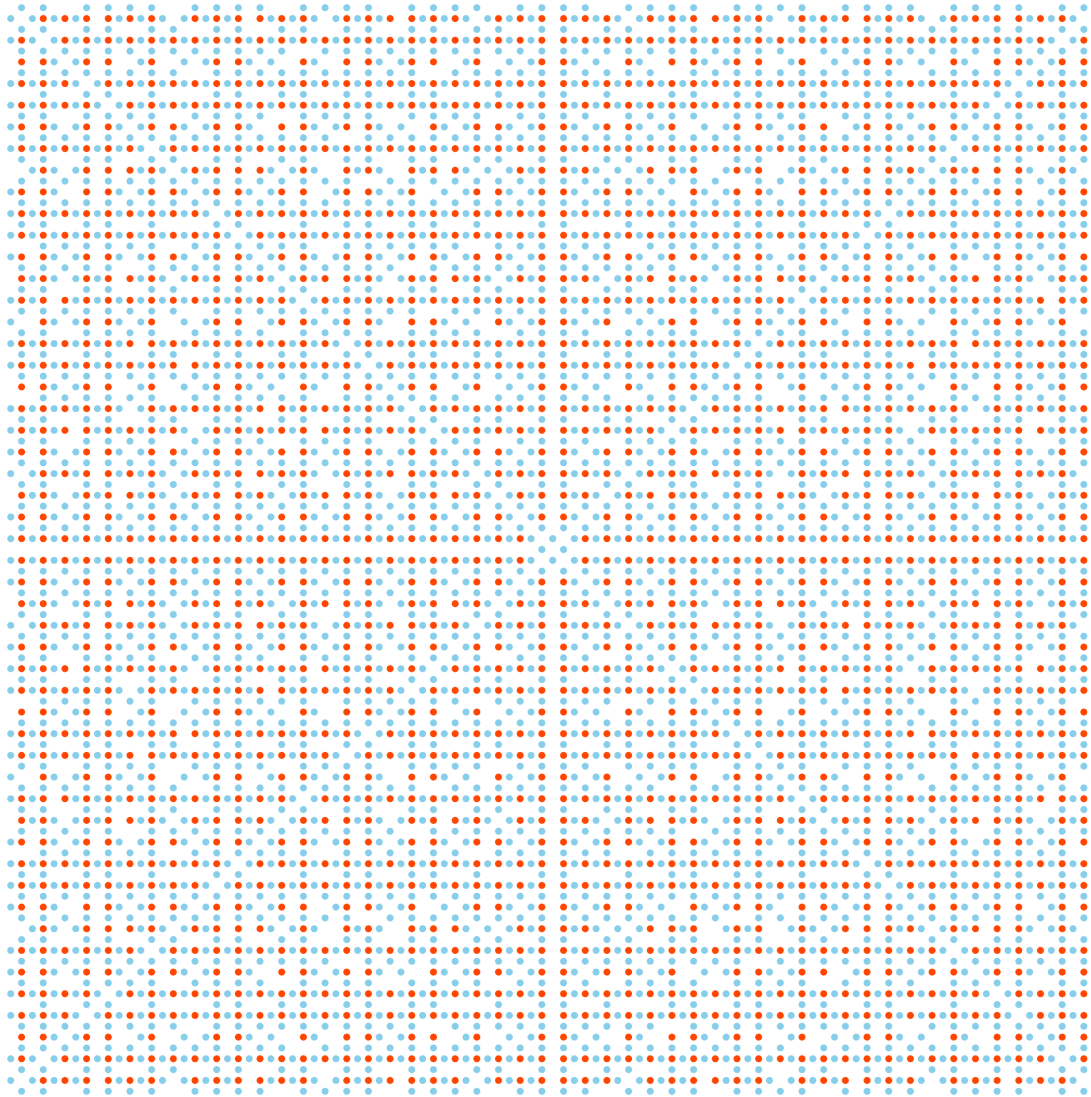


Figure: Partition of the set $\mathcal{V}(\mathbb{Z}) = \mathcal{V}(\mathbb{Z})_1 \sqcup \mathcal{V}(\mathbb{Z})_2$.

Step 3: sieving

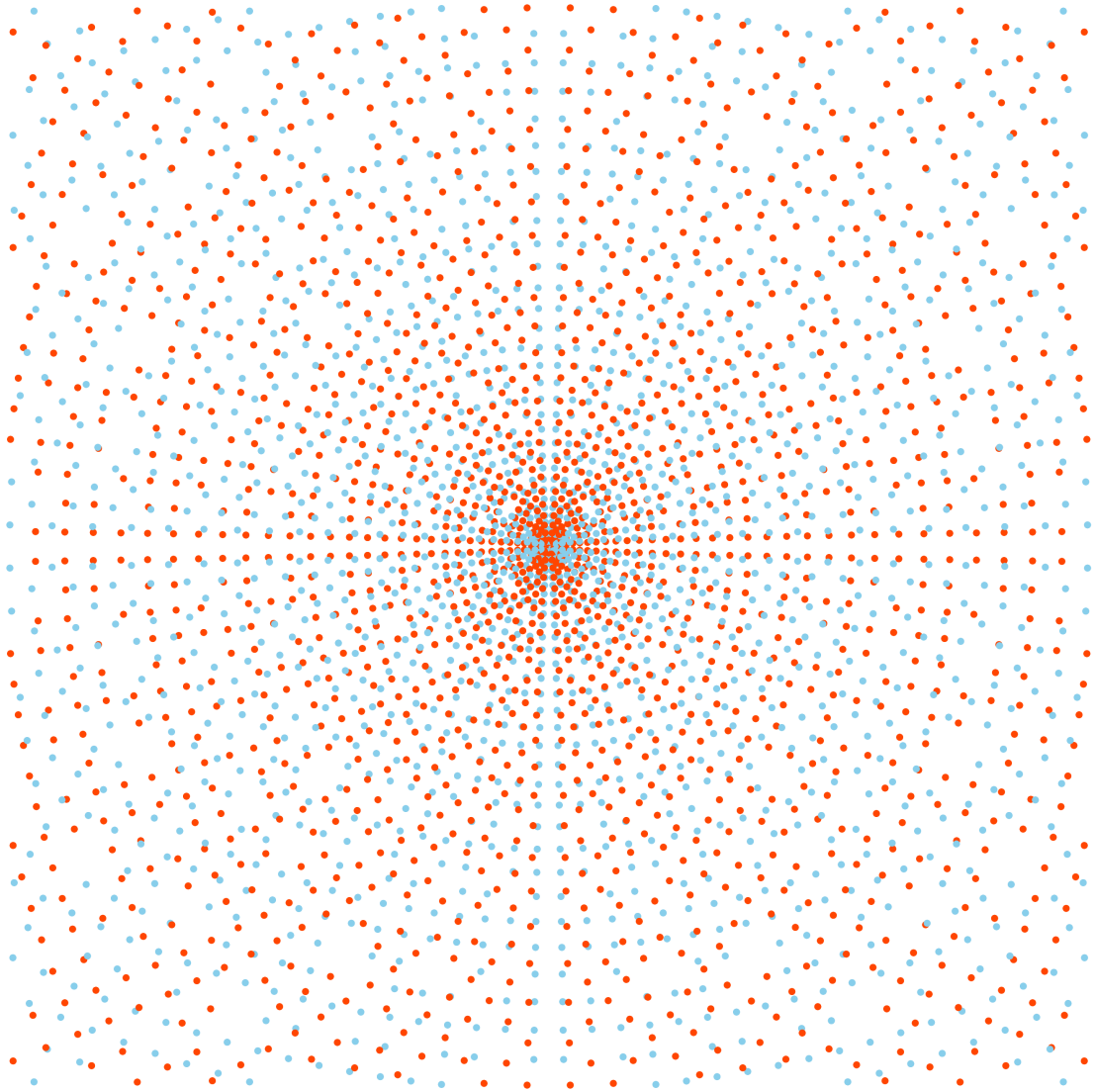


Figure: Partition of the set $\mathcal{U}(\mathbb{Z}) = \mathcal{U}(\mathbb{Z})_1 \sqcup \mathcal{U}(\mathbb{Z})_{-1} \sqcup \mathcal{U}(\mathbb{Z})_2 \sqcup \mathcal{U}(\mathbb{Z})_{-2}$.

The graded ring

$F = c_1x_1^{e_1} + c_2x_2^{e_2} + c_3x_3^{e_3}$, the $c_i \in \mathbb{Z}$

$\mathbf{e} := (e_1, e_2, e_3)$, the exponents vector

$m := \gcd(e_2e_3, e_1e_3, e_1e_2)$, $d := \gcd(e_1, e_2, e_3)$

$\mathbf{w} := (w_1, w_2, w_3) = \frac{1}{m}(e_2e_3, e_1e_3, e_1e_2)$, the weights vector

$\mathcal{R} := \mathbb{Z}[x_1, x_2, x_3]/\langle F \rangle$ graded ring $\deg x_i = w_i$

$\mathcal{R}^+$ the irrelevant ideal

Example

If $\mathbf{e} = (n, n, n)$, then $\mathbf{w} = (1, 1, 1)$.
If $\mathbf{e} = (a, a, c)$ for $a \nmid c$, then $m = a$ and $\mathbf{w} = (c, c, a)$.
If $\mathbf{e} = (a, a, a^v m)$ for $a \nmid m$ and $v \geqslant 1$, then $m = a^2$ and $\mathbf{w} = (a^{v-1}m, a^{v-1}m, 1)$.
If $\mathbf{e} = (2, 3, 7)$, then $m = 1$ and $\mathbf{w} = (21, 14, 6)$.

The graded ring

$F = c_1 x_1^{e_1} + c_2 x_2^{e_2} + c_3 x_3^{e_3}$, the $c_i \in \mathbb{Z}$

$\mathbf{e} := (e_1, e_2, e_3)$, the exponents vector

$m := \gcd(e_2 e_3, e_1 e_3, e_1 e_2)$, $d := \gcd(e_1, e_2, e_3)$

$\mathbf{w} := (w_1, w_2, w_3) = \frac{1}{m}(e_2 e_3, e_1 e_3, e_1 e_2)$, the weights vector

$\mathcal{R} := \mathbb{Z}[x_1, x_2, x_3]/\langle F \rangle$ graded ring $\deg x_i = w_i$

$\mathcal{R}^+$ the irrelevant ideal

Example

If $\mathbf{e} = (n, n, n)$, then $\mathbf{w} = (1, 1, 1)$.
If $\mathbf{e} = (a, a, c)$ for $a \nmid c$, then $m = a$ and $\mathbf{w} = (c, c, a)$.
If $\mathbf{e} = (a, a, a^v m)$ for $a \nmid m$ and $v \geqslant 1$, then $m = a^2$ and $\mathbf{w} = (a^{v-1} m, a^{v-1} m, 1)$.
If $\mathbf{e} = (2, 3, 7)$, then $m = 1$ and $\mathbf{w} = (21, 14, 6)$.

The graded ring

$F = c_1 x_1^{e_1} + c_2 x_2^{e_2} + c_3 x_3^{e_3}$, the $c_i \in \mathbb{Z}$

$\mathbf{e} := (e_1, e_2, e_3)$, the exponents vector

$m := \gcd(e_2 e_3, e_1 e_3, e_1 e_2)$, $d := \gcd(e_1, e_2, e_3)$

$\mathbf{w} := (w_1, w_2, w_3) = \frac{1}{m}(e_2 e_3, e_1 e_3, e_1 e_2)$, the weights vector

$\mathcal{R} := \mathbb{Z}[x_1, x_2, x_3]/\langle F \rangle$ graded ring $\deg x_i = w_i$

$\mathcal{R}^+$ the irrelevant ideal

Example

If $\mathbf{e} = (n, n, n)$, then $\mathbf{w} = (1, 1, 1)$.
If $\mathbf{e} = (a, a, c)$ for $a \nmid c$, then $m = a$ and $\mathbf{w} = (c, c, a)$.
If $\mathbf{e} = (a, a, a^v m)$ for $a \nmid m$ and $v \geqslant 1$, then $m = a^2$ and $\mathbf{w} = (a^{v-1} m, a^{v-1} m, 1)$.
If $\mathbf{e} = (2, 3, 7)$, then $m = 1$ and $\mathbf{w} = (21, 14, 6)$.

The graded ring

$F = c_1x_1^{e_1} + c_2x_2^{e_2} + c_3x_3^{e_3}$, the $c_i \in \mathbb{Z}$

$\mathbf{e} := (e_1, e_2, e_3)$, the exponents vector

$m := \gcd(e_2e_3, e_1e_3, e_1e_2)$, $d := \gcd(e_1, e_2, e_3)$

$\mathbf{w} := (w_1, w_2, w_3) = \frac{1}{m}(e_2e_3, e_1e_3, e_1e_2)$, the weights vector

$\mathcal{R} := \mathbb{Z}[x_1, x_2, x_3]/\langle F \rangle$ graded ring $\deg x_i = w_i$

$\mathcal{R}^+$ the irrelevant ideal

Example

If $\mathbf{e} = (n, n, n)$, then $\mathbf{w} = (1, 1, 1)$.
If $\mathbf{e} = (a, a, c)$ for $a \nmid c$, then $m = a$ and $\mathbf{w} = (c, c, a)$.
If $\mathbf{e} = (a, a, a^v m)$ for $a \nmid m$ and $v \geqslant 1$, then $m = a^2$ and $\mathbf{w} = (a^{v-1}m, a^{v-1}m, 1)$.
If $\mathbf{e} = (2, 3, 7)$, then $m = 1$ and $\mathbf{w} = (21, 14, 6)$.

The graded ring

$F = c_1x_1^{e_1} + c_2x_2^{e_2} + c_3x_3^{e_3}$, the $c_i \in \mathbb{Z}$

$\mathbf{e} := (e_1, e_2, e_3)$, the exponents vector

$m := \gcd(e_2e_3, e_1e_3, e_1e_2)$, $d := \gcd(e_1, e_2, e_3)$

$\mathbf{w} := (w_1, w_2, w_3) = \frac{1}{m}(e_2e_3, e_1e_3, e_1e_2)$, the weights vector

$\mathcal{R} := \mathbb{Z}[x_1, x_2, x_3]/\langle F \rangle$ graded ring $\deg x_i = w_i$

$\mathcal{R}^+$ the irrelevant ideal

Example

If $\mathbf{e} = (n, n, n)$, then $\mathbf{w} = (1, 1, 1)$.
If $\mathbf{e} = (a, a, c)$ for $a \nmid c$, then $m = a$ and $\mathbf{w} = (c, c, a)$.
If $\mathbf{e} = (a, a, a^v m)$ for $a \nmid m$ and $v \geqslant 1$, then $m = a^2$ and $\mathbf{w} = (a^{v-1}m, a^{v-1}m, 1)$.
If $\mathbf{e} = (2, 3, 7)$, then $m = 1$ and $\mathbf{w} = (21, 14, 6)$.

The graded ring

$F = c_1x_1^{e_1} + c_2x_2^{e_2} + c_3x_3^{e_3}$, the $c_i \in \mathbb{Z}$

$\mathbf{e} := (e_1, e_2, e_3)$, the exponents vector

$m := \gcd(e_2e_3, e_1e_3, e_1e_2)$, $d := \gcd(e_1, e_2, e_3)$

$\mathbf{w} := (w_1, w_2, w_3) = \frac{1}{m}(e_2e_3, e_1e_3, e_1e_2)$, the weights vector

$\mathcal{R} := \mathbb{Z}[x_1, x_2, x_3]/\langle F \rangle$ graded ring $\deg x_i = w_i$

$\mathcal{R}^+$ the irrelevant ideal

Example

If $\mathbf{e} = (n, n, n)$, then $\mathbf{w} = (1, 1, 1)$.
If $\mathbf{e} = (a, a, c)$ for $a \nmid c$, then $m = a$ and $\mathbf{w} = (c, c, a)$.
If $\mathbf{e} = (a, a, a^v m)$ for $a \nmid m$ and $v \geqslant 1$, then $m = a^2$ and $\mathbf{w} = (a^{v-1}m, a^{v-1}m, 1)$.
If $\mathbf{e} = (2, 3, 7)$, then $m = 1$ and $\mathbf{w} = (21, 14, 6)$.

The graded ring

$F = c_1 x_1^{e_1} + c_2 x_2^{e_2} + c_3 x_3^{e_3}$, the $c_i \in \mathbb{Z}$

$\mathbf{e} := (e_1, e_2, e_3)$, the exponents vector

$m := \gcd(e_2 e_3, e_1 e_3, e_1 e_2)$, $d := \gcd(e_1, e_2, e_3)$

$\mathbf{w} := (w_1, w_2, w_3) = \frac{1}{m}(e_2 e_3, e_1 e_3, e_1 e_2)$, the weights vector

$\mathcal{R} := \mathbb{Z}[x_1, x_2, x_3]/\langle F \rangle$ graded ring $\deg x_i = w_i$

$\mathcal{R}^+$ the irrelevant ideal

Example

If $\mathbf{e} = (n, n, n)$, then $\mathbf{w} = (1, 1, 1)$.
If $\mathbf{e} = (a, a, c)$ for $a \nmid c$, then $m = a$ and $\mathbf{w} = (c, c, a)$.
If $\mathbf{e} = (a, a, a^v m)$ for $a \nmid m$ and $v \geqslant 1$, then $m = a^2$ and $\mathbf{w} = (a^{v-1} m, a^{v-1} m, 1)$.
If $\mathbf{e} = (2, 3, 7)$, then $m = 1$ and $\mathbf{w} = (21, 14, 6)$.

The punctured cone

$\mathcal{U} := \operatorname{Spec} \mathcal{R} - V(\mathcal{R}^+) \subset \mathbb{A}^3_{\mathbb{Z}}$

It is a quasi-affine scheme of relative dimension 2 over $\mathbb{Z}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive integral solutions to $F = 0$

$\mathbb{G}_{\mathsf{m}} := \operatorname{Spec} \mathbb{Z}[u, u^{-1}]$ acts on $\mathcal{U}$ via

$$\lambda \cdot (x_1, x_2, x_3) := (\lambda^{w_1} x_1, \lambda^{w_2} x_2, \lambda^{w_3} x_3).$$

We consider the following subgroup schemes of the split torus $\mathsf{T} := \mathbb{G}_{\mathsf{m}} \times \mathbb{G}_{\mathsf{m}} \times \mathbb{G}_{\mathsf{m}}$:

$$\mathsf{I} := \operatorname{image}(\lambda \mapsto (\lambda^{w_1}, \lambda^{w_2}, \lambda^{w_3})),$$
$$H := \operatorname{Stab}_{\mathsf{T}}(\mathcal{U}).$$

The punctured cone

$$\mathcal{U} := \operatorname{Spec} \mathcal{R} - V(\mathcal{R}^+) \subset \mathbb{A}^3_{\mathbb{Z}}$$

It is a quasi-affine scheme of relative dimension 2 over $\mathbb{Z}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive integral solutions to $F = 0$

$\mathbb{G}_{\mathsf{m}} := \operatorname{Spec} \mathbb{Z}[u, u^{-1}]$ acts on $\mathcal{U}$ via

$$\lambda \cdot (x_1, x_2, x_3) := (\lambda^{w_1} x_1, \lambda^{w_2} x_2, \lambda^{w_3} x_3).$$

We consider the following subgroup schemes of the split torus $\mathsf{T} := \mathbb{G}_{\mathsf{m}} \times \mathbb{G}_{\mathsf{m}} \times \mathbb{G}_{\mathsf{m}}$:

$$\mathsf{I} := \operatorname{image}(\lambda \mapsto (\lambda^{w_1}, \lambda^{w_2}, \lambda^{w_3})),$$
$$H := \operatorname{Stab}_{\mathsf{T}}(\mathcal{U}).$$

The punctured cone

$\mathcal{U} := \operatorname{Spec} \mathcal{R} - V(\mathcal{R}^+) \subset \mathbb{A}^3_{\mathbb{Z}}$

It is a quasi-affine scheme of relative dimension 2 over $\mathbb{Z}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive integral solutions to $F = 0$

$\mathbb{G}_m := \operatorname{Spec} \mathbb{Z}[u, u^{-1}]$ acts on $\mathcal{U}$ via

$$\lambda \cdot (x_1, x_2, x_3) := (\lambda^{w_1} x_1, \lambda^{w_2} x_2, \lambda^{w_3} x_3).$$

We consider the following subgroup schemes of the split torus $\mathsf{T} := \mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m$:

$$\mathsf{I} := \operatorname{image}(\lambda \mapsto (\lambda^{w_1}, \lambda^{w_2}, \lambda^{w_3})),$$
$$H := \operatorname{Stab}_{\mathsf{T}}(\mathcal{U}).$$

The punctured cone

$\mathcal{U} := \operatorname{Spec} \mathcal{R} - V(\mathcal{R}^+) \subset \mathbb{A}^3_{\mathbb{Z}}$

It is a quasi-affine scheme of relative dimension 2 over $\mathbb{Z}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive integral solutions to $F = 0$

$\mathbb{G}_m := \operatorname{Spec} \mathbb{Z}[u, u^{-1}]$ acts on $\mathcal{U}$ via

$$\lambda \cdot (x_1, x_2, x_3) := (\lambda^{w_1} x_1, \lambda^{w_2} x_2, \lambda^{w_3} x_3).$$

We consider the following subgroup schemes of the split torus $\mathsf{T} := \mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m$:

$$\mathsf{I} := \operatorname{image}(\lambda \mapsto (\lambda^{w_1}, \lambda^{w_2}, \lambda^{w_3})),$$
$$H := \operatorname{Stab}_{\mathsf{T}}(\mathcal{U}).$$

The punctured cone

$\mathcal{U} := \operatorname{Spec} \mathcal{R} - V(\mathcal{R}^+) \subset \mathbb{A}^3_{\mathbb{Z}}$

It is a quasi-affine scheme of relative dimension 2 over $\mathbb{Z}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive integral solutions to $F = 0$

$\mathbb{G}_{\mathsf{m}} := \operatorname{Spec} \mathbb{Z}[u, u^{-1}]$ acts on $\mathcal{U}$ via

$$\lambda \cdot (x_1, x_2, x_3) := (\lambda^{w_1} x_1, \lambda^{w_2} x_2, \lambda^{w_3} x_3).$$

We consider the following subgroup schemes of the split torus $\mathsf{T} := \mathbb{G}_{\mathsf{m}} \times \mathbb{G}_{\mathsf{m}} \times \mathbb{G}_{\mathsf{m}}$:

$$\mathsf{I} := \operatorname{image}(\lambda \mapsto (\lambda^{w_1}, \lambda^{w_2}, \lambda^{w_3})),$$
$$H := \operatorname{Stab}_{\mathsf{T}}(\mathcal{U}).$$

The punctured cone

$\mathcal{U} := \operatorname{Spec} \mathcal{R} - V(\mathcal{R}^+) \subset \mathbb{A}^3_{\mathbb{Z}}$

It is a quasi-affine scheme of relative dimension 2 over $\mathbb{Z}$

$\mathcal{U}(\mathbb{Z})$ is the set of primitive integral solutions to $F = 0$

$\mathbb{G}_{\mathsf{m}} := \operatorname{Spec} \mathbb{Z}[u, u^{-1}]$ acts on $\mathcal{U}$ via

$$\lambda \cdot (x_1, x_2, x_3) := (\lambda^{w_1} x_1, \lambda^{w_2} x_2, \lambda^{w_3} x_3).$$

We consider the following subgroup schemes of the split torus $\mathsf{T} := \mathbb{G}_{\mathsf{m}} \times \mathbb{G}_{\mathsf{m}} \times \mathbb{G}_{\mathsf{m}}$:

$$\mathsf{I} := \operatorname{image}(\lambda \mapsto (\lambda^{w_1}, \lambda^{w_2}, \lambda^{w_3})),$$
$$H := \operatorname{Stab}_{\mathsf{T}}(\mathcal{U}).$$

The Fermat stack

$\mathscr{F} := [\mathcal{U}/_{\mathbf{w}}\mathbb{G}_{\mathsf{m}}] = [\mathcal{U}/\mathsf{I}]$

$\mathscr{F}$ is a closed substack of the weighted projective stack $\mathscr{P}(\mathbf{w})$

Lemma

If R is a principal ideal domain, $\mathcal{U}(R)/\mathsf{I}(R) \cong \mathscr{F}\langle R\rangle$.

Proof: By the method of descent wrt $j : \mathcal{U} \to [\mathcal{U}/I]$,

$$\mathscr{F}\langle R\rangle = \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathsf{I})} j^\tau(\mathcal{U}^\tau(R)).$$

But $\mathrm{H}^1(R,\mathsf{I}) \cong \mathrm{H}^1(R,\mathbb{G}_{\mathsf{m}}) = \mathrm{Pic}(R)$ is trivial. Thus every R-point of $\mathscr{F}$ comes from $\mathcal{U}(R)$.

$$\begin{array}{ccc} \mathsf{I} & \longrightarrow & \mathcal{U} \\ \downarrow & & \downarrow j \\ \operatorname{Spec} R & \dashrightarrow & \mathscr{F} \end{array}$$

□

The Fermat stack

$$\mathscr{F} := [\mathcal{U}/_{\mathbf{w}}\mathbb{G}_{\mathsf{m}}] = [\mathcal{U}/\mathsf{I}]$$

$\mathscr{F}$ is a closed substack of the weighted projective stack $\mathscr{P}(\mathbf{w})$

Lemma

If R is a principal ideal domain, $\mathcal{U}(R)/\mathsf{I}(R) \cong \mathscr{F}\langle R\rangle$.

Proof: By the method of descent wrt $j : \mathcal{U} \to [\mathcal{U}/I]$,

$$\mathscr{F}\langle R\rangle = \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathsf{I})} j^\tau(\mathcal{U}^\tau(R)).$$

But $\mathrm{H}^1(R,\mathsf{I}) \cong \mathrm{H}^1(R,\mathbb{G}_{\mathsf{m}}) = \mathrm{Pic}(R)$ is trivial. Thus every R-point of $\mathscr{F}$ comes from $\mathcal{U}(R)$.

$$\begin{array}{ccc} \mathsf{I} & \longrightarrow & \mathcal{U} \\ \downarrow & & \downarrow j \\ \operatorname{Spec} R & \dashrightarrow & \mathscr{F} \end{array}$$

□

The Fermat stack

$\mathscr{F} := [\mathcal{U}/_{\mathbf{w}}\mathbb{G}_{\mathsf{m}}] = [\mathcal{U}/\mathsf{I}]$

$\mathscr{F}$ is a closed substack of the weighted projective stack $\mathscr{P}(\mathbf{w})$

Lemma

If R is a principal ideal domain, $\mathcal{U}(R)/\mathsf{I}(R) \cong \mathscr{F}\langle R\rangle$.

Proof: By the method of descent wrt $j : \mathcal{U} \to [\mathcal{U}/I]$,

$$\mathscr{F}\langle R\rangle = \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathsf{I})} j^\tau(\mathcal{U}^\tau(R)).$$

But $\mathrm{H}^1(R,\mathsf{I}) \cong \mathrm{H}^1(R,\mathbb{G}_{\mathsf{m}}) = \mathrm{Pic}(R)$ is trivial. Thus every R-point of $\mathscr{F}$ comes from $\mathcal{U}(R)$.

$$\begin{array}{ccc} \mathsf{I} & \longrightarrow & \mathcal{U} \\ \downarrow & & \downarrow j \\ \operatorname{Spec} R & \dashrightarrow & \mathscr{F} \end{array}$$

□

The Fermat stack

$\mathscr{F} := [\mathcal{U}/_{\mathbf{w}}\mathbb{G}_{\mathsf{m}}] = [\mathcal{U}/\mathsf{I}]$

$\mathscr{F}$ is a closed substack of the weighted projective stack $\mathscr{P}(\mathbf{w})$

Lemma

If R is a principal ideal domain, $\mathcal{U}(R)/\mathsf{I}(R) \cong \mathscr{F}\langle R\rangle$.

Proof: By the method of descent wrt $j : \mathcal{U} \to [\mathcal{U}/I]$,

$$\mathscr{F}\langle R\rangle = \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathsf{I})} j^\tau(\mathcal{U}^\tau(R)).$$

But $\mathrm{H}^1(R,\mathsf{I}) \cong \mathrm{H}^1(R,\mathbb{G}_{\mathsf{m}}) = \mathrm{Pic}(R)$ is trivial. Thus every R-point of $\mathscr{F}$ comes from $\mathcal{U}(R)$.

$$\begin{array}{ccc} \mathsf{I} & \longrightarrow & \mathcal{U} \\ \downarrow & & \downarrow j \\ \operatorname{Spec} R & \dashrightarrow & \mathscr{F} \end{array}$$

□

The Fermat stack

$\mathscr{F} := [\mathcal{U}/_{\mathbf{w}}\mathbb{G}_{\mathsf{m}}] = [\mathcal{U}/\mathsf{I}]$

$\mathscr{F}$ is a closed substack of the weighted projective stack $\mathscr{P}(\mathbf{w})$

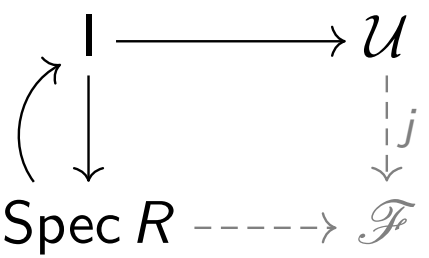
Lemma

If R is a principal ideal domain, $\mathcal{U}(R)/\mathsf{I}(R) \cong \mathscr{F}\langle R\rangle$.

Proof: By the method of descent wrt $j\colon \mathcal{U} \to [\mathcal{U}/I]$,

$$\mathscr{F}\langle R\rangle = \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathsf{I})} j^\tau(\mathcal{U}^\tau(R)).$$

But $\mathrm{H}^1(R,\mathsf{I}) \cong \mathrm{H}^1(R,\mathbb{G}_{\mathsf{m}}) = \mathrm{Pic}(R)$ is trivial. Thus every R-point of $\mathscr{F}$ comes from $\mathcal{U}(R)$.



□

The Belyi stack

$F = c_1 x_1^{e_1} + c_2 x_2^{e_2} + c_3 x_3^{e_3}$

$\mathscr{X} := [\mathcal{U}/\mathrm{H}]$

Lemma

If R is a principal ideal domain, $\mathcal{U}(R)/\mathrm{H}(R) \hookrightarrow \mathscr{X}\langle R\rangle$.

$L\colon c_1 y_1 + c_2 y_2 + c_3 y_3 \subset \mathbb{P}^2_{\mathbb{Z}}$, the line associated to F

Let $P_i := \{y_i = 0\} \in \mathrm{Div}(L)$

Lemma

$\mathscr{X}$ is isomorphic to the iterated root stack

$$\sqrt[e_1]{L; P_1} \times_L \sqrt[e_2]{L; P_2} \times_L \sqrt[e_3]{L; P_3}.$$

In particular, if R is a PID

$$\mathscr{X}\langle R\rangle \cong \left\{(y_1 : y_2 : y_3) \in L(R) : \text{the ideal } \langle y_i\rangle \text{ is an } e_i^{th} \text{ power}\right\}.$$

The Belyi stack

Σ_F set of primes dividing the e_i and c_i

Let $R = \mathbb{Z}[1/\Sigma_F]$ be the ring of Σ_F-integers of $\mathbb{Q}$

Lemma

After base change to R, $\mathscr{X}$ is isomorphic to the iterated root stack

$$\mathbb{P}^1(\mathbf{e}) := \sqrt[e_1]{\mathbb{P}^1; 0} \times_{\mathbb{P}^1} \sqrt[e_2]{\mathbb{P}^1; 1} \times_{\mathbb{P}^1} \sqrt[e_3]{\mathbb{P}^1; \infty}.$$

Proof idea: It suffices to find an isomorphism of the coarse spaces $L \to \mathbb{P}^1$ sending (P_1, P_2, P_3) to $(0, 1, \infty)$. After base change to R, the map $(y_1 : y_2 : y_3) \mapsto (-c_1 y_1 : c_3 y_3)$ works. $\square$

The Belyi stack

Σ_F set of primes dividing the e_i and c_i

Let $R = \mathbb{Z}[1/\Sigma_F]$ be the ring of Σ_F-integers of $\mathbb{Q}$

Lemma

After base change to R, $\mathscr{X}$ is isomorphic to the iterated root stack

$$\mathbb{P}^1(\mathbf{e}) := \sqrt[e_1]{\mathbb{P}^1; 0} \times_{\mathbb{P}^1} \sqrt[e_2]{\mathbb{P}^1; 1} \times_{\mathbb{P}^1} \sqrt[e_3]{\mathbb{P}^1; \infty}.$$

Proof idea: It suffices to find an isomorphism of the coarse spaces $L \to \mathbb{P}^1$ sending (P_1, P_2, P_3) to $(0, 1, \infty)$. After base change to R, the map $(y_1 : y_2 : y_3) \mapsto (-c_1 y_1 : c_3 y_3)$ works. $\square$

The Belyi stack

Σ_F set of primes dividing the e_i and c_i

Let $R = \mathbb{Z}[1/\Sigma_F]$ be the ring of Σ_F-integers of $\mathbb{Q}$

Lemma

After base change to R, $\mathscr{X}$ is isomorphic to the iterated root stack

$$\mathbb{P}^1(\mathbf{e}) := \sqrt[e_1]{\mathbb{P}^1; 0} \times_{\mathbb{P}^1} \sqrt[e_2]{\mathbb{P}^1; 1} \times_{\mathbb{P}^1} \sqrt[e_3]{\mathbb{P}^1; \infty}.$$

Proof idea: It suffices to find an isomorphism of the coarse spaces $L \to \mathbb{P}^1$ sending (P_1, P_2, P_3) to $(0, 1, \infty)$. After base change to R, the map $(y_1 : y_2 : y_3) \mapsto (-c_1 y_1 : c_3 y_3)$ works. $\square$

The Belyi stack

Σ_F set of primes dividing the e_i and c_i

Let $R = \mathbb{Z}[1/\Sigma_F]$ be the ring of Σ_F-integers of $\mathbb{Q}$

Lemma

After base change to R, $\mathscr{X}$ is isomorphic to the iterated root stack

$$\mathbb{P}^1(\mathbf{e}) := \sqrt[e_1]{\mathbb{P}^1; 0} \times_{\mathbb{P}^1} \sqrt[e_2]{\mathbb{P}^1; 1} \times_{\mathbb{P}^1} \sqrt[e_3]{\mathbb{P}^1; \infty}.$$

Proof idea: It suffices to find an isomorphism of the coarse spaces $L \to \mathbb{P}^1$ sending (P_1, P_2, P_3) to $(0, 1, \infty)$. After base change to R, the map $(y_1 : y_2 : y_3) \mapsto (-c_1 y_1 : c_3 y_3)$ works. $\square$

The Belyi stack

Σ_F set of primes dividing the e_i and c_i

Let $R = \mathbb{Z}[1/\Sigma_F]$ be the ring of Σ_F-integers of $\mathbb{Q}$

Lemma

After base change to R, $\mathscr{X}$ is isomorphic to the iterated root stack

$$\mathbb{P}^1(\mathbf{e}) := \sqrt[e_1]{\mathbb{P}^1; 0} \times_{\mathbb{P}^1} \sqrt[e_2]{\mathbb{P}^1; 1} \times_{\mathbb{P}^1} \sqrt[e_3]{\mathbb{P}^1; \infty}.$$

Proof idea: It suffices to find an isomorphism of the coarse spaces $L \to \mathbb{P}^1$ sending (P_1, P_2, P_3) to $(0, 1, \infty)$. After base change to R, the map $(y_1 : y_2 : y_3) \mapsto (-c_1 y_1 : c_3 y_3)$ works. $\square$

Belyi maps

k a number field

$\varphi\colon Z \to \mathbb{P}^1$ a k-Belyi map

We say that φ is Galois if the monodromy group $\mathrm{Aut}(\varphi)(\bar{k})$ acts transitively on $\varphi^{-1}\{0,1,\infty\} \subset Z(\bar{k})$.

This is the case if and only if $\#\,\mathrm{Aut}(\varphi)(\bar{k}) = \deg\varphi$.

The signature of a Galois Belyi map $\varphi\colon Z \to \mathbb{P}^1$ is the triple (e_0, e_1, e_∞) where e_P is the ramification index $e_\varphi(z)$ of any critical point $z \in Z$ with critical value $P \in \{0,1,\infty\}$.

Belyi maps

k a number field

$\varphi\colon Z \to \mathbb{P}^1$ a k-Belyi map

We say that φ is Galois if the monodromy group $\mathrm{Aut}(\varphi)(\bar{k})$ acts transitively on $\varphi^{-1}\{0,1,\infty\} \subset Z(\bar{k})$.

This is the case if and only if $\#\,\mathrm{Aut}(\varphi)(\bar{k}) = \deg\varphi$.

The signature of a Galois Belyi map $\varphi\colon Z \to \mathbb{P}^1$ is the triple (e_0, e_1, e_∞) where e_P is the ramification index $e_\varphi(z)$ of any critical point $z \in Z$ with critical value $P \in \{0,1,\infty\}$.

Belyi maps

k a number field

$\varphi\colon Z \to \mathbb{P}^1$ a k-Belyi map

We say that φ is Galois if the monodromy group $\mathrm{Aut}(\varphi)(\bar{k})$ acts transitively on $\varphi^{-1}\{0,1,\infty\} \subset Z(\bar{k})$.

This is the case if and only if $\#\,\mathrm{Aut}(\varphi)(\bar{k}) = \deg\varphi$.

The signature of a Galois Belyi map $\varphi\colon Z \to \mathbb{P}^1$ is the triple (e_0, e_1, e_∞) where e_P is the ramification index $e_\varphi(z)$ of any critical point $z \in Z$ with critical value $P \in \{0,1,\infty\}$.

Belyi maps

k a number field

$\varphi\colon Z \to \mathbb{P}^1$ a k-Belyi map

We say that φ is Galois if the monodromy group $\mathrm{Aut}(\varphi)(\bar{k})$ acts transitively on $\varphi^{-1}\{0,1,\infty\} \subset Z(\bar{k})$.

This is the case if and only if $\#\,\mathrm{Aut}(\varphi)(\bar{k}) = \deg\varphi$.

The signature of a Galois Belyi map $\varphi\colon Z \to \mathbb{P}^1$ is the triple (e_0, e_1, e_∞) where e_P is the ramification index $e_\varphi(z)$ of any critical point $z \in Z$ with critical value $P \in \{0,1,\infty\}$.

Belyi maps

k a number field

$\varphi\colon Z \to \mathbb{P}^1$ a k-Belyi map

We say that φ is Galois if the monodromy group $\mathrm{Aut}(\varphi)(\bar{k})$ acts transitively on $\varphi^{-1}\{0,1,\infty\} \subset Z(\bar{k})$.

This is the case if and only if $\#\,\mathrm{Aut}(\varphi)(\bar{k}) = \deg\varphi$.

The signature of a Galois Belyi map $\varphi\colon Z \to \mathbb{P}^1$ is the triple (e_0, e_1, e_∞) where e_P is the ramification index $e_\varphi(z)$ of any critical point $z \in Z$ with critical value $P \in \{0,1,\infty\}$.

Belyi maps

k a number field

$\varphi\colon Z \to \mathbb{P}^1$ a k-Belyi map

We say that φ is Galois if the monodromy group $\mathrm{Aut}(\varphi)(\bar{k})$ acts transitively on $\varphi^{-1}\{0,1,\infty\} \subset Z(\bar{k})$.

This is the case if and only if $\#\,\mathrm{Aut}(\varphi)(\bar{k}) = \deg\varphi$.

The signature of a Galois Belyi map $\varphi\colon Z \to \mathbb{P}^1$ is the triple (e_0, e_1, e_∞) where e_P is the ramification index $e_\varphi(z)$ of any critical point $z \in Z$ with critical value $P \in \{0,1,\infty\}$.

Key fact 1

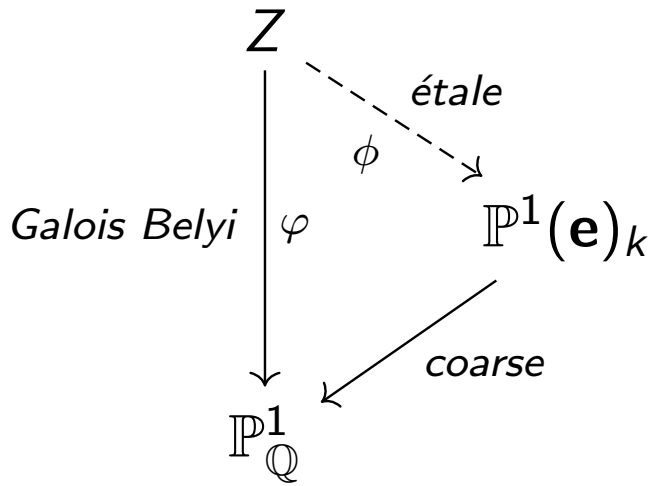
Lemma

Every Galois Belyi map $\varphi\colon Z \to \mathbb{P}^1_k$ of signature $\mathbf{e}$ factors through the coarse space map $\mathbb{P}^1(\mathbf{e})_k \to \mathbb{P}^1_k$

Key fact 1

Lemma

Every Galois Belyi map $\varphi\colon Z \to \mathbb{P}^1_k$ *of signature* $\mathbf{e}$ *factors through the coarse space map* $\mathbb{P}^1(\mathbf{e})_k \to \mathbb{P}^1_k$



Key fact 2

Lemma

For $\mathbf{e}$ *spherical, there exists a Galois Belyi map* $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ *of signature* $\mathbf{e}$*, which is defined over* $\mathbb{Q}$*, and*

$$\deg \varphi = |G| = 2/\chi(\mathbf{e})$$

Furthermore, there exists a finite set of bad places Σ *of* $\mathbb{Q}$*, such that* φ *can be spread out to the ring* R *of* Σ*-integers in* $\mathbb{Q}$*.*

Key fact 2

Lemma

For $\mathbf{e}$ *spherical, there exists a Galois Belyi map* $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ *of signature* $\mathbf{e}$*, which is defined over* $\mathbb{Q}$*, and*

$$\deg \varphi = |G| = 2/\chi(\mathbf{e})$$

Furthermore, there exists a finite set of bad places Σ *of* $\mathbb{Q}$*, such that* φ *can be spread out to the ring* R *of* Σ*-integers in* $\mathbb{Q}$*.*

Main theorem

$F := Ax^a + By^b + Cz^c$

$\chi(F) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$

$N(F, H)$: the number of primitive integral solutions (x, y, z) to $F = 0$ with $\mathrm{Ht}_{\mathbb{P}^1}(Ax^a : Cz^c) \leqslant H$.

Theorem (A-P)

Suppose that $\chi > 0$ and that $\mathcal{U}(\mathbb{Z}) \neq \emptyset$. Then, there exists an effectively computable constant $\kappa(F) > 0$ such that

$$N(F, H) \sim \kappa(F) \cdot H^{\chi}, \quad \text{as} \quad H \to \infty.$$

Proof sketch of main theorem

For a subset $\Omega \subset \mathbb{P}^1(\mathbb{Q})$, let

$$N(\Omega, h) := \#\left\{P \in \Omega : \mathrm{Ht}_{\mathbb{P}^1}(P) \leqslant h\right\}.$$

1. Use the isomorphism $\mathscr{X}_R \to \mathbb{P}^1(\mathbf{e})_R$ and first estimate $N(\mathscr{X}\langle R\rangle, h)$.
2. From the "key facts", we can write $\mathbb{P}^1(\mathbf{e})_R \cong [\mathbb{P}^1_R/\mathcal{G}]$.
3. By the method of descent,

$$\mathscr{X}\langle R\rangle \cong \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathcal{G})} \phi_\tau(\mathbb{P}^1_\tau(R)) = \bigsqcup_{\tau \in \mathrm{H}^1_\Sigma(\mathbb{Q},G)} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).$$

4. The maps $\phi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1(\mathbf{e})_\mathbb{Q}$ give rise to Galois Belyi maps $\varphi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1$, defined over $\mathbb{Q}$.

Proof sketch of main theorem

For a subset $\Omega \subset \mathbb{P}^1(\mathbb{Q})$, let

$$N(\Omega, h) := \#\left\{P \in \Omega : \mathrm{Ht}_{\mathbb{P}^1}(P) \leqslant h\right\}.$$

1. Use the isomorphism $\mathscr{X}_R \to \mathbb{P}^1(\mathbf{e})_R$ and first estimate $N(\mathscr{X}\langle R\rangle, h)$.
2. From the "key facts", we can write $\mathbb{P}^1(\mathbf{e})_R \cong [\mathbb{P}^1_R/\mathcal{G}]$.
3. By the method of descent,

$$\mathscr{X}\langle R\rangle \cong \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathcal{G})} \phi_\tau(\mathbb{P}^1_\tau(R)) = \bigsqcup_{\tau \in \mathrm{H}^1_\Sigma(\mathbb{Q},G)} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).$$

4. The maps $\phi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1(\mathbf{e})_\mathbb{Q}$ give rise to Galois Belyi maps $\varphi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1$, defined over $\mathbb{Q}$.

Proof sketch of main theorem

For a subset $\Omega \subset \mathbb{P}^1(\mathbb{Q})$, let

$$N(\Omega, h) := \#\left\{P \in \Omega : \mathrm{Ht}_{\mathbb{P}^1}(P) \leqslant h\right\}.$$

1. Use the isomorphism $\mathscr{X}_R \to \mathbb{P}^1(\mathbf{e})_R$ and first estimate $N(\mathscr{X}\langle R\rangle, h)$.
2. From the "key facts", we can write $\mathbb{P}^1(\mathbf{e})_R \cong [\mathbb{P}^1_R/\mathcal{G}]$.
3. By the method of descent,

$$\mathscr{X}\langle R\rangle \cong \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathcal{G})} \phi_\tau(\mathbb{P}^1_\tau(R)) = \bigsqcup_{\tau \in \mathrm{H}^1_\Sigma(\mathbb{Q},G)} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).$$

4. The maps $\phi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1(\mathbf{e})_\mathbb{Q}$ give rise to Galois Belyi maps $\varphi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1$, defined over $\mathbb{Q}$.

Proof sketch of main theorem

For a subset $\Omega \subset \mathbb{P}^1(\mathbb{Q})$, let

$$N(\Omega, h) := \#\left\{P \in \Omega : \mathrm{Ht}_{\mathbb{P}^1}(P) \leqslant h\right\}.$$

1. Use the isomorphism $\mathscr{X}_R \to \mathbb{P}^1(\mathbf{e})_R$ and first estimate $N(\mathscr{X}\langle R\rangle, h)$.
2. From the "key facts", we can write $\mathbb{P}^1(\mathbf{e})_R \cong [\mathbb{P}^1_R/\mathcal{G}]$.
3. By the method of descent,

$$\mathscr{X}\langle R\rangle \cong \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathcal{G})} \phi_\tau(\mathbb{P}^1_\tau(R)) = \bigsqcup_{\tau \in \mathrm{H}^1_\Sigma(\mathbb{Q},G)} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).$$

4. The maps $\phi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1(\mathbf{e})_\mathbb{Q}$ give rise to Galois Belyi maps $\varphi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1$, defined over $\mathbb{Q}$.

Proof sketch of main theorem

For a subset $\Omega \subset \mathbb{P}^1(\mathbb{Q})$, let

$$N(\Omega, h) := \#\left\{P \in \Omega : \mathrm{Ht}_{\mathbb{P}^1}(P) \leqslant h\right\}.$$

1. Use the isomorphism $\mathscr{X}_R \to \mathbb{P}^1(\mathbf{e})_R$ and first estimate $N(\mathscr{X}\langle R\rangle, h)$.
2. From the "key facts", we can write $\mathbb{P}^1(\mathbf{e})_R \cong [\mathbb{P}^1_R/\mathcal{G}]$.
3. By the method of descent,

$$\mathscr{X}\langle R\rangle \cong \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathcal{G})} \phi_\tau(\mathbb{P}^1_\tau(R)) = \bigsqcup_{\tau \in \mathrm{H}^1_\Sigma(\mathbb{Q},G)} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).$$

4. The maps $\phi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1(\mathbf{e})_\mathbb{Q}$ give rise to Galois Belyi maps $\varphi_\tau : \mathbb{P}^1_\tau \to \mathbb{P}^1$, defined over $\mathbb{Q}$.

Proof sketch of main theorem

For a subset $\Omega \subset \mathbb{P}^1(\mathbb{Q})$, let

$$N(\Omega, h) := \#\left\{P \in \Omega : \mathrm{Ht}_{\mathbb{P}^1}(P) \leqslant h\right\}.$$

1. Use the isomorphism $\mathscr{X}_R \to \mathbb{P}^1(\mathbf{e})_R$ and first estimate $N(\mathscr{X}\langle R\rangle, h)$.
2. From the "key facts", we can write $\mathbb{P}^1(\mathbf{e})_R \cong [\mathbb{P}^1_R/\mathcal{G}]$.
3. By the method of descent,

$$\mathscr{X}\langle R\rangle \cong \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathcal{G})} \phi_\tau(\mathbb{P}^1_\tau(R)) = \bigsqcup_{\tau \in \mathrm{H}^1_\Sigma(\mathbb{Q},G)} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).$$

4. The maps $\phi_\tau \colon \mathbb{P}^1_\tau \to \mathbb{P}^1(\mathbf{e})_\mathbb{Q}$ give rise to Galois Belyi maps $\varphi_\tau \colon \mathbb{P}^1_\tau \to \mathbb{P}^1$, defined over $\mathbb{Q}$.

Proof sketch of main theorem

For a subset $\Omega \subset \mathbb{P}^1(\mathbb{Q})$, let

$$N(\Omega, h) := \#\left\{P \in \Omega : \mathrm{Ht}_{\mathbb{P}^1}(P) \leqslant h\right\}.$$

1. Use the isomorphism $\mathscr{X}_R \to \mathbb{P}^1(\mathbf{e})_R$ and first estimate $N(\mathscr{X}\langle R\rangle, h)$.
2. From the "key facts", we can write $\mathbb{P}^1(\mathbf{e})_R \cong [\mathbb{P}^1_R/\mathcal{G}]$.
3. By the method of descent,

$$\mathscr{X}\langle R\rangle \cong \bigsqcup_{\tau \in \mathrm{H}^1(R,\mathcal{G})} \phi_\tau(\mathbb{P}^1_\tau(R)) = \bigsqcup_{\tau \in \mathrm{H}^1_\Sigma(\mathbb{Q},G)} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).$$

4. The maps $\phi_\tau \colon \mathbb{P}^1_\tau \to \mathbb{P}^1(\mathbf{e})_\mathbb{Q}$ give rise to Galois Belyi maps $\varphi_\tau \colon \mathbb{P}^1_\tau \to \mathbb{P}^1$, defined over $\mathbb{Q}$.

Proof sketch of main theorem

5. $N(\mathscr{X}\langle R\rangle, h) = \sum_\tau N(\varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h)$.
6. Each $N(\phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h) \sim \kappa_\tau \cdot H^{2/\deg \varphi_\tau} = \kappa_\tau \cdot H^\chi$ and $\kappa_\tau = 0$ iff $\mathbb{P}^1_\tau$ is a pointless conic.
7. Use that $\mathcal{U}(R)/\mathrm{H}(R) \hookrightarrow \mathscr{X}\langle R\rangle$ and the estimate $N(\mathscr{X}\langle R\rangle, h)$ to recover $N(\mathcal{U}(R)/\mathrm{H}(R), h)$.
8. Argue that $\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}) \hookrightarrow \mathcal{U}(R)/\mathrm{H}(R)$ has positive density.
9. Conclude from $N(F, h) = N(\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}), h)$.

Proof sketch of main theorem

5. $N(\mathscr{X}\langle R\rangle, h) = \sum_\tau N(\varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h)$.
6. Each $N(\phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h) \sim \kappa_\tau \cdot H^{2/\deg \varphi_\tau} = \kappa_\tau \cdot H^\chi$ and $\kappa_\tau = 0$ iff $\mathbb{P}^1_\tau$ is a pointless conic.
7. Use that $\mathcal{U}(R)/\mathrm{H}(R) \hookrightarrow \mathscr{X}\langle R\rangle$ and the estimate $N(\mathscr{X}\langle R\rangle, h)$ to recover $N(\mathcal{U}(R)/\mathrm{H}(R), h)$.
8. Argue that $\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}) \hookrightarrow \mathcal{U}(R)/\mathrm{H}(R)$ has positive density.
9. Conclude from $N(F, h) = N(\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}), h)$.

Proof sketch of main theorem

5. $N(\mathscr{X}\langle R\rangle, h) = \sum_\tau N(\varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h)$.
6. Each $N(\phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h) \sim \kappa_\tau \cdot H^{2/\deg \varphi_\tau} = \kappa_\tau \cdot H^\chi$ and $\kappa_\tau = 0$ iff $\mathbb{P}^1_\tau$ is a pointless conic.
7. Use that $\mathcal{U}(R)/\mathrm{H}(R) \hookrightarrow \mathscr{X}\langle R\rangle$ and the estimate $N(\mathscr{X}\langle R\rangle, h)$ to recover $N(\mathcal{U}(R)/\mathrm{H}(R), h)$.
8. Argue that $\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}) \hookrightarrow \mathcal{U}(R)/\mathrm{H}(R)$ has positive density.
9. Conclude from $N(F, h) = N(\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}), h)$.

Proof sketch of main theorem

5. $N(\mathscr{X}\langle R\rangle, h) = \sum_\tau N(\varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h)$.
6. Each $N(\phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h) \sim \kappa_\tau \cdot H^{2/\deg \varphi_\tau} = \kappa_\tau \cdot H^\chi$ and $\kappa_\tau = 0$ iff $\mathbb{P}^1_\tau$ is a pointless conic.
7. Use that $\mathcal{U}(R)/\mathrm{H}(R) \hookrightarrow \mathscr{X}\langle R\rangle$ and the estimate $N(\mathscr{X}\langle R\rangle, h)$ to recover $N(\mathcal{U}(R)/\mathrm{H}(R), h)$.
8. Argue that $\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}) \hookrightarrow \mathcal{U}(R)/\mathrm{H}(R)$ has positive density.
9. Conclude from $N(F, h) = N(\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}), h)$.

Proof sketch of main theorem

5. $N(\mathscr{X}\langle R\rangle, h) = \sum_\tau N(\varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h)$.
6. Each $N(\phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h) \sim \kappa_\tau \cdot H^{2/\deg \varphi_\tau} = \kappa_\tau \cdot H^\chi$ and $\kappa_\tau = 0$ iff $\mathbb{P}^1_\tau$ is a pointless conic.
7. Use that $\mathcal{U}(R)/\mathrm{H}(R) \hookrightarrow \mathscr{X}\langle R\rangle$ and the estimate $N(\mathscr{X}\langle R\rangle, h)$ to recover $N(\mathcal{U}(R)/\mathrm{H}(R), h)$.
8. Argue that $\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}) \hookrightarrow \mathcal{U}(R)/\mathrm{H}(R)$ has positive density.
9. Conclude from $N(F, h) = N(\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}), h)$.

Proof sketch of main theorem

5. $N(\mathscr{X}\langle R\rangle, h) = \sum_\tau N(\varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h)$.
6. Each $N(\phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})), h) \sim \kappa_\tau \cdot H^{2/\deg \varphi_\tau} = \kappa_\tau \cdot H^\chi$ and $\kappa_\tau = 0$ iff $\mathbb{P}^1_\tau$ is a pointless conic.
7. Use that $\mathcal{U}(R)/\mathrm{H}(R) \hookrightarrow \mathscr{X}\langle R\rangle$ and the estimate $N(\mathscr{X}\langle R\rangle, h)$ to recover $N(\mathcal{U}(R)/\mathrm{H}(R), h)$.
8. Argue that $\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}) \hookrightarrow \mathcal{U}(R)/\mathrm{H}(R)$ has positive density.
9. Conclude from $N(F, h) = N(\mathcal{U}(\mathbb{Z})/\mathrm{H}(\mathbb{Z}), h)$.

Future work

1. Write a computer program that receives a GFE satisfying $\chi > 0$, and outputs the parametrization of its primitive solutions.
2. Write a computer program that receives a GFE satisfying $\chi = 0$, and outputs the parametrization of its primitive solutions. (In this case, the corresponding Belyi stack is covered by genus one curves).

Future work

1. Write a computer program that receives a GFE satisfying $\chi > 0$, and outputs the parametrization of its primitive solutions.
2. Write a computer program that receives a GFE satisfying $\chi = 0$, and outputs the parametrization of its primitive solutions. (In this case, the corresponding Belyi stack is covered by genus one curves).

Future work

1. Write a computer program that receives a GFE satisfying $\chi > 0$, and outputs the parametrization of its primitive solutions.
2. Write a computer program that receives a GFE satisfying $\chi = 0$, and outputs the parametrization of its primitive solutions. (In this case, the corresponding Belyi stack is covered by genus one curves).

Future work

1. Write a computer program that receives a GFE satisfying $\chi > 0$, and outputs the parametrization of its primitive solutions.
2. Write a computer program that receives a GFE satisfying $\chi = 0$, and outputs the parametrization of its primitive solutions. (In this case, the corresponding Belyi stack is covered by genus one curves).

Counting rational points on genus zero modular curves

Theorem (A-P, Han, Padurariu, Park)

There exist explicitly computable constants $C_5, C_5', C_5'' \in \mathbb{R}$ *and* $c_5 \in (0,1)$ *such that*

$$N_5(h) = C_5 h^{1/6} (\log h)^2 + C_5' h^{1/6} (\log h) + C_5'' h^{1/6} + O\left(\frac{h^{1/6}}{(\log h)^{c_5}}\right),$$

as $h \to \infty$. *Furthermore, the constant* C_5 *is given by*

$$C_5 = \frac{41}{1536\pi} \cdot V_5 \cdot g_1,$$

where V_5 *is the volume of an explicit region, and* g_1 *is given by*

$$g_1 = \frac{48}{\pi^4} \prod_{p \equiv 1 \bmod 4} \left(1 - \frac{4}{(p+1)^2}\right).$$

Counting rational points on genus zero modular curves

Theorem (A-P, Han, Padurariu, Park)

There exist explicitly computable constants $C_5, C_5', C_5'' \in \mathbb{R}$ *and* $c_5 \in (0,1)$ *such that*

$$N_5(h) = C_5 h^{1/6} (\log h)^2 + C_5' h^{1/6} (\log h) + C_5'' h^{1/6} + O\left(\frac{h^{1/6}}{(\log h)^{c_5}} \right),$$

as $h \to \infty$. *Furthermore, the constant* C_5 *is given by*

$$C_5 = \frac{41}{1536\pi} \cdot V_5 \cdot g_1,$$

where V_5 *is the volume of an explicit region, and* g_1 *is given by*

$$g_1 = \frac{48}{\pi^4} \prod_{p \equiv 1 \bmod 4} \left(1 - \frac{4}{(p+1)^2}\right).$$

Thanks!

Figure: June 2023 at Niagara Falls. (MRC workshop: *Explicit computations with stacks*).