Distribution Agreement

Generalized Fermat equations, stacks, and arithmetic statistics

By

Santiago Arango-Piñeros
Doctor of Philosophy

Mathematics

David Zureick-Brown, Ph.D.
Advisor 1

John Voight, Ph.D.
Advisor 2

David Borthwick, Ph.D.
Committee Member

Suresh Venapally, Ph.D.
Committee Member

Bjorn Poonen, Ph.D.
Committee Member

Accepted:

Kimberly Jacob Arriola, PhD.
Dean of the James T. Laney School of Graduate Studies

Date

Generalized Fermat equations, stacks, and arithmetic statistics

By

Santiago Arango-Piñeros
B.S., Universidad de los Andes, Bogotá, Colombia, 2017
M.Sc., Instituto de Matemática Pura e Aplicada, Rio de Janeiro, Brazil, 2019

Advisors: David Zureick-Brown, Ph.D. and John Voight, Ph.D.

An abstract of
A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2025

Abstract

Generalized Fermat equations, stacks, and arithmetic statistics
By Santiago Arango-Piñeros

Let (a, b, c) be a triple of positive integers. The *Belyi stack* $\mathbb{P}^1(a, b, c)$ is the algebraic stack obtained by rooting the projective line at $0, 1$, and ∞ with multiplicities a, b, and c, respectively.

In this thesis, we study the relationship between primitive integral solutions to generalized Fermat equations

$$F\colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0 \tag{1}$$

and the $\mathcal{S}$-integral points on $\mathbb{P}^1(a, b, c)$.

We find that, after inverting a suitable finite set $\mathcal{S}$ of rational primes, the stack $\mathbb{P}^1(a, b, c)$ is isomorphic to the quotient $[\mathcal{U}/\mathsf{H}]$, where $\mathcal{U}$ is the punctured cone defined by F, and H is the stabilizer group scheme of $\mathcal{U}$ in $\mathbb{G}_{\mathrm{m}}^3$. By descent theory, the $\mathcal{S}$-integral points of $\mathbb{P}^1(a, b, c)$ are partitioned into $\mathsf{H}(\mathbb{Z}_{\mathcal{S}})$-orbits of $\mathcal{U}_\tau(\mathbb{Z}_{\mathcal{S}})$ for an explicit set of twists F_τ of Equation (1). From this perspective, we reformulate the proofs of the landmark results of Darmon–Granville [13, Theorem 2] and Beukers [7, Theorem 1.2].

Finally, we obtain a winsome application in arithmetic statistics. Suppose that the Euler characteristic $\chi(F) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$ is positive, and that there exists at least one primitive integral solution to Equation (1). Then, we prove that there is an explicitly computable constant $\kappa(F) > 0$ such that the number of primitive integral solutions (x, y, z) to Equation (1) of height $\max\{|Ax^a|, |Cz^c|\}$ not exceeding h is asymptotic to $\kappa(F) \cdot h^{\chi}$.

Generalized Fermat equations, stacks, and arithmetic statistics

By

Santiago Arango-Piñeros
B.S., Universidad de los Andes, Bogotá, Colombia, 2017
M.Sc., Instituto de Matemática Pura e Aplicada, Rio de Janeiro, Brazil, 2019

Advisors: David Zureick-Brown, Ph.D. and John Voight, Ph.D.

A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2025

Acknowledgments

First, I thank David Zureick-Brown. You have been a constant source of inspiration and support. Thank you for patiently answering my questions and for believing in my potential. I look forward to moving to Amherst and finally seeing you in person again! Second, I thank John Voight. You have been a wonderful mentor—thank you for thoughtfully responding to my emails, providing detailed feedback, and generously sharing your ideas. You always go above and beyond; traveling from Sydney to Atlanta for my defense is just one example. Thanks also to Andrew Kobin for the Friday GFE meetings and for your thoughtful feedback on an earlier draft. I'm also grateful to Bjorn Poonen for serving on my committee—I greatly appreciate your detailed and insightful feedback.

I'm deeply thankful to my friends and collaborators for their time, support, and teachings. Special thanks to Alexis Newton for our coffee study sessions; Robert Hernandez and Jasmine Camero for our taco nights; Chris Keyes and Daniel Keliher for the fun times; Sam Frengley for recommending descent theory; Sun Woo Park for being the best; and Sameera Vemulapalli for teaching me the importance of **deeply** understanding basic examples.

During my PhD, I was fortunate to meet many inspiring mathematicians who inspired me to work hard and occasionally shared valuable words of wisdom. In particular, thanks to Alina Bucur, Francesc Fité, Sachi Hashimoto, Borys Kadets, Aaron Landesman, Robert Lemke Oliver, Soumya Sankar, Padmavathi Srinivasan, Frank Thorne, and Isabel Vogt. Special thanks to Jordan Ellenberg and Kiran Kedlaya for their guidance and for agreeing to write recommendation letters on my behalf.

Finalmente, debo reconocer que todo se lo debo a mi familia. Poncho y Carola, los amo con todo mi corazón; gracias por todo. Feli[1], Nanis y Mari, gracias por siempre estar ahí para apoyarme. Nico y Pau, gracias por abrirme las puertas de su casa en Boston. Gracias a Juan por las aventuras rockeras. Luisfer y Helen, muchas gracias por ser mis fans. Avery, conocerte fue el descubrimiento más importante de mi doctorado. Muchas gracias por tu apoyo y compañía. Te amo.

[1]Gracias por enseñarme a completar cuadrados, bro.

Contents

1 Introduction **1**

1.1 Parametrizing Pythagorean triples via the method of Fermat descent 3

1.2 Counting integral points on the projective line with three fractional points . . . 9

2 Background **16**

2.1 The groupoid of points on a stack . . . 16

2.2 H^1, torsors, and quotient stacks . . . 18

2.2.1 Nonabelian Čech cohomology . . . 18

2.2.2 Torsor sheaves . . . 19

2.2.3 Torsor schemes . . . 21

2.2.4 Quotient stacks . . . 23

2.2.5 The method of descent . . . 24

2.3 The root stack construction . . . 28

2.3.1 Generalized effective Cartier divisors . . . 28

2.3.2 Definition of a root stack . . . 29

2.3.3 The projective line rooted at a point . . . 31

3 Stacks associated to generalized Fermat equations **35**

3.1 The projective line with three fractional points . . . 35

3.1.1 A brief discussion of triangle groups . . . 35

3.1.2 Existence of Galois Belyi maps 37
3.1.3 The Belyi stack 39
3.2 The Fermat stack 42
3.2.1 The graded ring 43
3.2.2 The stacky proj 45
3.3 The group scheme H 47
3.4 The Belyi stack as a quotient 50
3.5 The method of descent on the Belyi stack 54
3.5.1 The theorem of Darmon–Granville 55
3.5.2 The theorem of Beukers 56

4 Counting primitive integral solutions 58
4.1 Rational points of bounded height in the image of a rational function 58
4.1.1 The primitivity defect set 60
4.1.2 Proofs 62
4.2 Counting integral points on the Belyi stack 65
4.3 Counting primitive integral solutions to generalized Fermat equations 66

Bibliography 69

List of Figures

1.1 Partition of the set $\mathcal{V}(\mathbb{Z}) = \mathcal{V}(\mathbb{Z})_1 \sqcup \mathcal{V}(\mathbb{Z})_2$. 7

1.2 Visualization of the partition $\mathcal{U}(\mathbb{Z}) = \mathcal{U}(\mathbb{Z})_1 \sqcup \mathcal{U}(\mathbb{Z})_{-1} \sqcup \mathcal{U}(\mathbb{Z})_2 \sqcup \mathcal{U}(\mathbb{Z})_{-2}$. 8

2.1 Proof of the method of descent. 28

3.1 The Belyi stack of signature (a, b, c). 39

3.2 Generators of the fundamental group of the orbifold $\mathbb{P}^1(a, b, c)(\mathbb{C})$. . . 42

4.1 Partition $\mathcal{V}(\mathbb{Z}) = \mathcal{V}(\mathbb{Z})_1 \sqcup \mathcal{V}(\mathbb{Z})_4$ with respect to the map $\phi(s : t) = ((s^2 - t^2)^2 : (2st)^2)$, with primitivity defect set $\mathcal{D}(\phi) = \{1, 4\}$. 61

List of Tables

1.1 G-twists of Pythagorean equation. 12

3.1 Spherical triangle groups. 37

3.2 Examples of Galois $\mathbb{Q}$-Belyi maps for the spherical signatures. 38

Chapter 1

Introduction

The main topic of this thesis is the study of integer solutions to Generalized Fermat equations. These are polynomial equations of the form the form

$$F\colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0 \tag{1.1}$$

where $A, B, C \in \mathbb{Z}$ satisfy $ABC \neq 0$. A solution $(x, y, z) \in \mathbb{Z}^3$ to Equation (1.1) is called primitive if the greatest common divisor of the triple is 1. We will focus on understanding the geometric structures that arise from the study of primitive integral solutions to Equation (1.1), rather than on the set of primitive solutions to any particular instance of the equation.

When the equation is homogeneous of degree n, it defines a smooth projective curve $C = \operatorname{Proj} \mathbb{Q}[\mathsf{x}, \mathsf{y}, \mathsf{z}]/\langle F \rangle$, and there is a two-to-one correspondence between the set of primitive integral solutions to Equation (1.1) and set of rational points $C(\mathbb{Q})$. When F is not homogeneous, we are led to study the integral points of a quasi-affine surface with complicated singularities. As stubborn enthusiasts of the arithmetic of algebraic curves, we are inspired by the following quote from Henri Darmon [12] on this subject.

"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."

The notion of curves with multiplicities introduced by Darmon coincides with the notion of relative stacky curves, as defined in [38] by Voight and Zureick-Brown, and the language of stacks provides a more conceptual framework that allows one to apply familiar geometric methods to this more general context. Indeed, the classical method of descent (arguably discovered by Fermat himself) can be extended to this context, and has been applied with great success by Poonen, Schaefer, and Stoll [30] to find the sixteen primitive integral solutions to $x^2 + y^3 - z^7 = 0$.

The contents of this work are organized as follows:

- In Chapter 2, we summarize the necessary background from the theory of stacks. We follow closely the conventions in Olsson's book [25]. The emphasis is on understanding the arithmetic of the stacks under consideration; i.e., their groupoids of integral and rational points. In the case of quotient stacks, the main tool is the method of descent described in Section 2.2.5. The main results of this chapter are Theorem 2.2.5.d, and the explicit calculation of the set of PID points on the projective line rooted at a point Proposition 2.3.3.d.

- In Chapter 3, we introduce the relevant geometric structures that arise from the study of primitive integral solutions. As an application, we provide a reformulation of the classical results of Darmon–Granville [13, Theorem 2] and Beukers [7, Theorem 1.2]. We hope that this chapter will serve as a useful reference for researchers interested in exploiting the stacky perspective in the study of generalized Fermat equations. This appears to be the first systematic study of generalized Fermat equations from the point of view of stacks, although experts have been aware of the connection for decades. Chapter 3 builds on the blueprints laid out by Poonen, Schaefer, and Stoll in [30], and by Poonen in [27] and [29]. Recently, Santens [31, 32] has developed part of the theory of relative (arithmetic) stacky curves that is essential for this work, and it appears that the study of generalized Fermat equations is also a primary motivation of his. Aside from the theory developed in this chapter, the main results are Theorem 3.4.0.b and Theorem 3.5.0.c.

- In Chapter 4 we focus on the arithmetic statistics of primitive integral solutions. We study the asymptotic count of solutions to those generalized Fermat equations that have infinitely many primitive integral solutions. Our approach uses the tools developed in the previous chapters. Our main theorem is Theorem 1.2.0.d (c.f. Theorem 4.3.0.b).

To introduce these ideas, we outline an application of the method of *Fermat descent* in the elementary case of the Pythagorean equation, where the use of stacks is not required and would be considered excessive. In Section 1.1 we explain how one could use this method to recover the known parametrizations. In Section 1.2 we introduce the integral points on the *Belyi stack* $\mathbb{P}^1(a,b,c)$, and relate our main result to the classical asymptotic counts of Pythagorean triples.

1.1 Parametrizing Pythagorean triples via the method of Fermat descent

It is a beautiful classical theorem that there are infinitely many primitive integral solutions to the Pythagorean equation $\mathsf{x}^2+\mathsf{y}^2-\mathsf{z}^2=0$. Furthermore, we understand how to parametrize its primitive integral solutions. Consider the polynomial functions

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

Theorem 1.1.0.a. *Every primitive integral solution* $(x, y, z) \in \mathbb{Z}^3$ *to the Diophantine equation* $\mathsf{x}^2 + \mathsf{y}^2 - \mathsf{z}^2 = 0$ *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* $s \not\equiv t \bmod 2$.

Elementary proofs of this theorem can be found in every introductory text in Number Theory. Line by line, these proofs clearly explain how the parametrizations arise. In the opinion of the author, however, the *why* remains mysterious.

Question 1.1.0.b. *Why is there a congruence condition specifically at the prime* 2*?*

Question 1.1.0.c. *What is the geometric origin of the parametrization?*

Question 1.1.0.d. *Where does the symmetry in the parametrization come from?*

We will attempt to answer all of these questions using the method of *Fermat descent*, a modern incarnation of Fermat's method of *infinite descent*. Our implementation of the method has three main steps: covering, twisting, and sieving.

Step 1: covering

Our task is to find a "covering" $\phi\colon \mathcal{V} \to \mathcal{U}$. Concretely, by a covering we mean a (right) fppf G-torsor $\phi\colon \mathcal{V} \to \mathcal{U}$, where G is some fppf group scheme over $\operatorname{Spec}\mathbb{Z}$. By the Hermite–Minkowski theorem (i.e., $\pi_1(\operatorname{Spec}\mathbb{Z}) = 1$) this is too much to ask, but it can be done if we allow ourselves to remove a finite set of bad primes.

Ideally, $\mathcal{V}$ will be a space that we understand well. In this case, we can let $\mathcal{V}$ be the punctured affine plane $\mathbb{A}^2 - \mathbf{0}$, as a scheme over the arithmetic line $\operatorname{Spec}\mathbb{Z}$. The set of integral points $\mathcal{V}(\mathbb{Z})$ is identified with the pairs $(s,t) \in \mathbb{Z}^2$ satisfying $\gcd(s,t) = 1$. Let $\mathcal{U}$ be the punctured cone, over $\operatorname{Spec}\mathbb{Z}$, corresponding to the Pythagorean equation $\mathsf{x}^2 + \mathsf{y}^2 - \mathsf{z}^2 = 0$. Similarly, the set of integral points $\mathcal{U}(\mathbb{Z})$ is identified with the primitive integral solutions to the Pythagorean equation. The group $\mu_2 \subset \mathbb{G}_{\mathrm{m}}$ inherits the diagonal action of $\mathbb{G}_{\mathrm{m}}$ on $\mathcal{V}$.

Lemma 1.1.0.e. *Let* $R = \mathbb{Z}[1/2]$. *The morphism* $\phi\colon \mathcal{V}_R \to \mathcal{U}_R$ *given by* $(\mathsf{s},\mathsf{t}) \mapsto (\mathsf{s}^2-\mathsf{t}^2, 2\mathsf{s}\mathsf{t}, \mathsf{s}^2+\mathsf{t}^2)$ *is an fppf* μ_2*-torsor.*

The proof of this lemma comes down to realizing that $R[\mathsf{s}^2-\mathsf{t}^2, 2\mathsf{s}\mathsf{t}, \mathsf{s}^2+\mathsf{t}^2] = R[\mathsf{s}^2, \mathsf{s}\mathsf{t}, \mathsf{t}^2]$ is the ring of invariants $R[\mathsf{s},\mathsf{t}]^{\{\pm 1\}}$. This statement is certainly false if we replace R by $\mathbb{Z}$, hinting a partial answer to Question 1.1.0.b: it seems that 2 shows up because the chosen map ϕ is not a "covering" unless we remove this prime.

Step 2: twisting

Descent theory tells us that once we have a covering, the points on the base are partitioned by the images of the points of the twists. In this particular situation, we have that

$$\mathcal{U}(R) = \bigsqcup_{\tau \in \mathrm{H}^1(R,\mu_2)} \phi_\tau(\mathcal{V}_\tau(R)).$$

To understand the right hand side, we first need to understand the Čech cohomology group $\mathrm{H}^1(R,\mu_2)$ classifying isomorphism classes of fppf μ_2-torsors over $\operatorname{Spec} R$. From the Kummer exact sequence, we see that $\mathrm{H}^1(R,\mu_2) \cong R^\times/(R^\times)^2 \cong \{\pm 1, \pm 2\}$. Concretely, to each $d \in \{\pm 1, \pm 2\}$ corresponds the μ_2-torsor $T_d := \operatorname{Spec} R[u]/\langle u^2 - d\rangle$. With this explicit description of the indexing set, the equation above now reads

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

The task at hand now is to compute the twists $\phi_d\colon \mathcal{V}_d \to \mathcal{U}$.

Lemma 1.1.0.f. *For* $d \in \{\pm 1, \pm 2\}$, *the twist* ϕ_d *of* ϕ *is given by* $\phi_d = \frac{1}{d}\phi\colon \mathcal{V} \to \mathcal{U}$.

Proof. First, recall that $\mathcal{V}_d$ is the quotient of $\mathcal{V} \times_R T_d$ by the twisted action of μ_2 given by $((\mathsf{s},\mathsf{t}),\sqrt{d}) \cdot \xi := ((\xi\mathsf{s},\xi\mathsf{t}),\xi\sqrt{d})$. Since the ring of invariants $(R[\mathsf{s},\mathsf{t}] \otimes_R R[\sqrt{d}])^{\{\pm 1\}}$

is isomorphic to $R[\sqrt{d}\mathsf{s}, \sqrt{d}\mathsf{t}]$, we see that after extending the base to T_d, we have an isomorphism $\psi_d \colon \mathcal{V}_{R[\sqrt{d}]} \to (\mathcal{V}_d)_{R[\sqrt{d}]}$ given by $(\mathsf{s}, \mathsf{t}) \mapsto (\sqrt{d}\mathsf{s}, \sqrt{d}\mathsf{t})$. We use ψ_d to identify $\mathcal{V}$ with $\mathcal{V}_d$ and ϕ_d with $\frac{1}{d}\phi$. □

With this explicit description of the twists, the partition of $\mathcal{U}(R)$ given by descent theory now reads

$$\mathcal{U}(R) = \bigsqcup_{d \in \{\pm 1, \pm 2\}} \tfrac{1}{d}\phi(\mathcal{V}(R)). \tag{1.2}$$

Step 3: sieving

Since we are interested in the subset $\mathcal{U}(\mathbb{Z})$ of $\mathcal{U}(R)$, we must sieve away the excess of R-points. For example, we want to get rid of the point $\phi(-1, 3/2) = (-5/4, -3, 13/4) \in \mathcal{U}(R)$. With our current choices, we will see that it is enough to restrict the domain $\mathcal{V}(R)$ to certain subsets $\mathcal{V}(\mathbb{Z})_1, \mathcal{V}(\mathbb{Z})_2$ of $\mathcal{V}(\mathbb{Z})$ to hit all the primitive integral solutions to the Pythagorean equation. (Recall that the set $\mathcal{V}(R)$ consists of pairs $(s,t) \in R^2$ generating the trivial ideal: $sR + tR = R$.) It is at this stage that the usual arguments from elementary number theory play a role.

Lemma 1.1.0.g. *If* $(s,t) \in \mathcal{V}(\mathbb{Z})$, *then* $\gcd(\phi(s,t)) \in \{1, 2\}$. *Moreover,* $\gcd(\phi(s,t)) = 2$ *if and only if* $s \equiv t \bmod 2$.

This lemma defines for us a partition $\mathcal{V}(\mathbb{Z}) = \mathcal{V}(\mathbb{Z})_1 \sqcup \mathcal{V}(\mathbb{Z})_2$, according to the greatest common divisor of the image of ϕ:

$$\mathcal{V}(\mathbb{Z})_{|d|} := \{(s,t) \in \mathcal{V}(\mathbb{Z}) : \gcd(\phi(s,t)) = |d|\}.$$

Let $(x, y, z) \in \mathcal{U}(\mathbb{Z})$, and define

$$d(x,y,z) := \begin{cases} \operatorname{sign}(z), & \text{if } x \equiv 1 \bmod 2, \\ \operatorname{sign}(z) \cdot 2, & \text{if } x \equiv 0 \bmod 2. \end{cases}$$

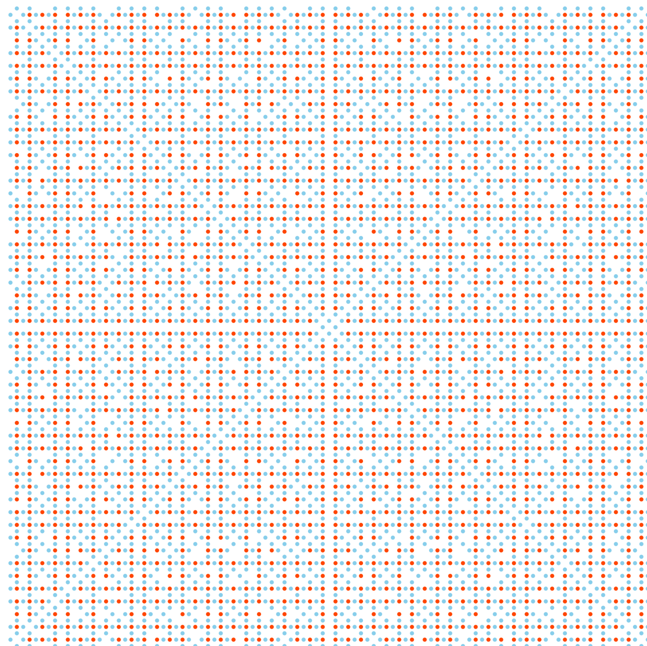


Figure 1.1: Partition of the set $\mathcal{V}(\mathbb{Z}) = \mathcal{V}(\mathbb{Z})_1 \sqcup \mathcal{V}(\mathbb{Z})_2$.

Partition $\mathcal{U}(\mathbb{Z})$ according to this invariant, so that

$$\mathcal{U}(\mathbb{Z}) = \mathcal{U}(\mathbb{Z})_1 \sqcup \mathcal{U}(\mathbb{Z})_{-1} \sqcup \mathcal{U}(\mathbb{Z})_2 \sqcup \mathcal{U}(\mathbb{Z})_{-2}.$$

It turns our that this naive partition of the set of primitive integral solutions has geometric meaning: it comes from the method of descent.

Lemma 1.1.0.h. *For each $d \in \{\pm 1, \pm 2\}$, we have that $\mathcal{U}(\mathbb{Z})_d = \mathcal{U}(\mathbb{Z}) \cap \phi_d(\mathcal{V}(R))$. Moreover,*

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

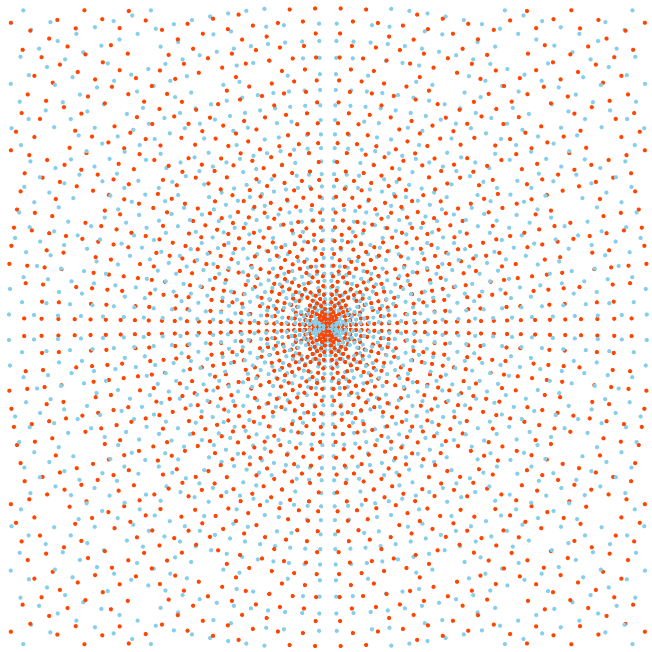


Figure 1.2: Visualization of the partition $\mathcal{U}(\mathbb{Z}) = \mathcal{U}(\mathbb{Z})_1 \sqcup \mathcal{U}(\mathbb{Z})_{-1} \sqcup \mathcal{U}(\mathbb{Z})_2 \sqcup \mathcal{U}(\mathbb{Z})_{-2}$.

Putting everything together, we have that

$$\begin{aligned}\mathcal{U}(\mathbb{Z}) &= \mathcal{U}(\mathbb{Z})_1 \sqcup \mathcal{U}(\mathbb{Z})_{-1} \sqcup \mathcal{U}(\mathbb{Z})_2 \sqcup \mathcal{U}(\mathbb{Z})_{-2} \\ &= \phi(\mathcal{V}(\mathbb{Z})_1) \sqcup -\phi(\mathcal{V}(\mathbb{Z})_1) \sqcup \hat{\phi}(\mathcal{V}(\mathbb{Z})_1) \sqcup -\hat{\phi}(\mathcal{V}(\mathbb{Z})_1),\end{aligned}$$

concluding the proof of Theorem 1.1.0.a. See Figure 1.2 for a visualization of the partition of primitive solutions arising from this choice of cover ϕ. (We are only plotting the points (x, y) corresponding to a triple $(x, y, \pm z)$.)

The point, of course, is that even though this is not the most economical way to solve the problem, the *method of descent* sketched here is more conceptual, and works (with some stacky input) when the Pythagorean equation is replaced by an arbitrary generalized Fermat equation $A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0$ with integer coefficients. We need only work over a stack that is birational to the projective line $\mathbb{P}^1_{\mathbb{Z}}$, but where the irreducible divisors 0, 1, and ∞ have been replaced by certain "fractions" of themselves.

1.2 Counting integral points on the projective line with three fractional points

We follow [27]. Let a, b, c be positive integers, and consider the following subset of the rational points on the projective line $\mathbb{P}^1(\mathbb{Q}) \cong \mathbb{Q} \cup \left\{\frac{1}{0}\right\}$.

$$\Omega(a,b,c) := \left\{ Q \in \mathbb{P}^1(\mathbb{Q}) : \begin{array}{l} \text{(i) num}(Q) \text{ is an } a^{\text{th}} \text{ power,} \\ \text{(ii) num}(Q-1) \text{ is a } b^{\text{th}} \text{ power,} \\ \text{(iii) den}(Q) \text{ is a } c^{\text{th}} \text{ power.} \end{array} \right\}. \tag{1.3}$$

By the numerator and denominator of a point $Q \in \mathbb{P}^1(\mathbb{Q})$, we mean the first and second coordinate of any representative $\pm(n, d) \in \mathbb{Z}^2$ for $Q = (n : d)$ with $\gcd(n, d) = 1$. This pair is only well defined up to sign. We say that an integer m is an n^{th} power if the ideal $m\mathbb{Z}$ equals $e^n\mathbb{Z}$ for some $e \geqslant 0$. In particular, $0, 1, \infty \in \Omega(a, b, c)$.

To any subset $\Omega \subseteq \mathbb{P}^1(\mathbb{Q})$ we associate the subset of points of bounded height, and the corresponding counting function. Given h positive, define

$$\Omega_{\leqslant h} := \{Q \in \Omega : \mathrm{Ht}(Q) \leqslant h\}, \quad N(\Omega; h) := \#\Omega_{\leqslant h}, \tag{1.4}$$

where $\mathrm{Ht}\colon \mathbb{P}^1(\mathbb{Q}) \to \mathbb{Z}_{\geqslant 0}$ is the usual multiplicative height, given by

$$\mathrm{Ht}(Q) = \max\{|\operatorname{num}(Q)|, |\operatorname{den}(Q)|\}. \tag{1.5}$$

Heuristic 1.2.0.a. We estimate the probability that a uniformly random rational number of height not exceeding $h \gg 0$ is in the set $\Omega(a, b, c)$. We do this under the heuristic assumption that the events (i), (ii), and (iii) defining $\Omega(a, b, c)$ in Equation (1.3) are *independent*.

We have that

$$\frac{\#\left\{Q \in \mathbb{P}^1(\mathbb{Q})_{\leqslant h} \colon \operatorname{num}(Q) \text{ is an } a^{\text{th}} \text{ power}\right\}}{\#\mathbb{P}^1(\mathbb{Q})_{\leqslant h}} \doteq \frac{h \cdot h^{1/a}}{h^2} = h^{-1+1/a},$$
$$\frac{\#\left\{Q \in \mathbb{P}^1(\mathbb{Q})_{\leqslant h} \colon \operatorname{num}(Q-1) \text{ is an } b^{\text{th}} \text{ power}\right\}}{\#\mathbb{P}^1(\mathbb{Q})_{\leqslant h}} \doteq \frac{h \cdot h^{1/b}}{h^2} = h^{-1+1/b},$$
$$\frac{\#\left\{Q \in \mathbb{P}^1(\mathbb{Q})_{\leqslant h} \colon \operatorname{den}(Q) \text{ is an } c^{\text{th}} \text{ power}\right\}}{\#\mathbb{P}^1(\mathbb{Q})_{\leqslant h}} \doteq \frac{h \cdot h^{1/c}}{h^2} = h^{-1+1/c},$$

where the notation $f(h) \doteq g(h)$ means that there exists an implicit constant $\kappa > 0$ such that $f(h) = \kappa \cdot g(h)$ as $h \to \infty$. The independence assumption implies that

$$\frac{\#\Omega(a,b,c)}{\#\mathbb{P}^1(\mathbb{Q})_{\leqslant h}} \doteq \left(h^{-1+1/a}\right)\left(h^{-1+1/b}\right)\left(h^{-1+1/c}\right) \doteq h^{-3+1/a+1/b+1/c}.$$

The heuristic above suggests that the Euler characteristic

$$\chi(a,b,c) := \tfrac{1}{a} + \tfrac{1}{b} + \tfrac{1}{c} - 1 \tag{1.6}$$

forces $\Omega(a,b,c)$ to be

$$\begin{cases} \text{infinite}, & \text{if } \chi(a,b,c) > 0, \text{ and} \\ \text{finite}, & \text{if } \chi(a,b,c) < 0. \end{cases}$$

This prediction turns out to be correct. The hyperbolic case (when $\chi < 0$) can be deduced from a theorem of Darmon and Granville [13, Theorem 2]. The spherical case (when $\chi > 0$) can be deduced from a theorem of Beukers [7, Theorem 1.2]. More precisely, the heuristic suggests that in the spherical case, $N(\Omega(a,b,c); h) \asymp h^{\chi}$.

Theorem 1.2.0.b. *Suppose that $a, b, c > 1$ and that $\chi := \chi(a,b,c) > 0$. Then, for* *every $\varepsilon > 0$, there exists an explicitly computable constant $\kappa(a,b,c) > 0$ such that*

$$N(\Omega(a,b,c),h) = \kappa(a,b,c) \cdot h^{\chi} + O(h^{\chi/2+\varepsilon}),$$

as $h \to \infty$. The implicit constant depends on (a,b,c) and ε.

Our approach is geometric: we use the method of descent on a certain stack $\mathbb{P}^1(a,b,c)$. We call it the Belyi stack of signature (a,b,c), primarily because étale covers $\phi\colon X \to \mathbb{P}^1(a,b,c)_{\mathbb{Q}}$ are in bijective correspondence with Belyi maps $\varphi\colon X \to \mathbb{P}^1_{\mathbb{Q}}$. The stack $\mathbb{P}^1(a,b,c)$ is birational to $\mathbb{P}^1_{\mathbb{Z}}$, but the irreducible divisors 0, 1, and ∞ have μ_a, μ_b, and μ_c automorphism groups, respectively. (Technically, $\mathbb{P}^1(a,b,c)$ is the iterated root stack of $\mathbb{P}^1_{\mathbb{Z}}$ along these divisors, with the corresponding multiplicities.)

The main point, hinted at by Poonen in [27], is that the set $\Omega(a,b,c) \subset \mathbb{P}^1(\mathbb{Q})$ we have been discussing coincides with the set of isomorphism classes of the groupoid of $\mathbb{Z}$-points on the stack $\mathbb{P}^1(a,b,c)$. It also coincides with the set of integral points on Darmon's M-curve $\mathbf{P}^1_{a,b,c}$, and, as Darmon remarks in [12], "up to some sloppiness in the signs," it also coincides with the set of primitive integral solutions to the equation $\mathsf{x}^a + \mathsf{y}^b + \mathsf{z}^c = 0$.

The case of signature $(a,b,c) = (2,2,2)$ will serve as a simple example to guide our intuition for the non-homogeneous spherical signatures. Lehmer [21, p. 38] and Lambek–Moser [20] counted the asymptotic number of Pythagorean triangles with bounded hypothenuse.

Consider the group $G := \{\pm 1\}^3 / \pm 1$, and note that G is isomorphic to the Klein four group. List its elements

$$\begin{aligned} e_0 &= [1,1,1], & e_1 &= [-1,1,1], \\ e_2 &= [1,-1,1], & e_3 &= [1,1,-1]. \end{aligned}$$

Consider the conics F_0, F_1, F_2, F_3 with coefficients given by element in G with matching index. For each element in G, we attach a corresponding j-map.

Table 1.1: G-twists of Pythagorean equation.

G	F	j
e_0	$\mathsf{x}^2+\mathsf{y}^2+\mathsf{z}^2=0$	$(x,y,z)\mapsto(-x^2:z^2)$
e_1	$\mathsf{x}^2-\mathsf{y}^2-\mathsf{z}^2=0$	$(x,y,z)\mapsto(x^2:z^2)$
e_2	$\mathsf{x}^2-\mathsf{y}^2+\mathsf{z}^2=0$	$(x,y,z)\mapsto(-x^2:z^2)$
e_3	$\mathsf{x}^2+\mathsf{y}^2-\mathsf{z}^2=0$	$(x,y,z)\mapsto(x^2:z^2)$

Theorem 1.2.0.c. *As $h\to\infty$, we have the asymptotic relation*

$$N(\Omega(2,2,2);h)\sim\tfrac{24}{\pi}\cdot h^{1/2}.$$

Moreover, the set $\Omega(2,2,2)$ is the pushout

$$\frac{\Omega(F_1)\sqcup\Omega(F_2)\sqcup\Omega(F_3)}{\{0,1,\infty\}}.$$

In other words, $\Omega(2,2,2)=\Omega(F_1)\cup\Omega(F_2)\cup\Omega(F_3)$ and the intersections $\Omega(F_i)\cap\Omega(F_j)$ are contained in $\{0,1,\infty\}$. From this description, we deduce that

$$N(\Omega(F_1);h)=N(\Omega(F_2);h)=N(\Omega(F_3);h)\sim\tfrac{8}{\pi}\cdot h^{1/2}.$$

Proof. The pushout description of $\Omega(2,2,2)$ follows by partitioning the set according to the signs of $\operatorname{num}(Q),\operatorname{num}(Q-1)$, and $\operatorname{den}(Q)$, and staring at Table 1.1.

Step 1: A suitable covering is readily available. Indeed, if $Z=Z_0$ denotes the plane conic defined by F_0, the j-map $j_0\colon\mathcal{U}_0\to\mathbb{P}^1$ induces the morphism

$$\phi\colon Z_0\to\mathbb{P}^1_{\mathbb{Q}},\quad (x:y:z)\mapsto(-x^2:z^2).$$

One verifies that ϕ is a Galois Belyi map defined over $\mathbb{Q}$ with Galois group G, diagonally embedded in $\mathrm{PGL}_3(\mathbb{Q})$. (Although any such cover $Z_i \to \mathbb{P}^1$ would suffice, we choose the pointless conic for dramatic emphasis.) Since $\mathcal{U}_0(\mathbb{Z})$ is empty, so is $\Omega(F_0)$.

Step 2: Consider the Galois cohomology group $\mathrm{H}^1(\mathbb{Q}, G)$. Since the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}}$ acts trivially on the abelian group G, $\mathrm{H}^1(\mathbb{Q}, G)$ is the group of continuous group homomorphisms $\mathrm{Gal}_{\mathbb{Q}} \to H$. Every such map factors through a unique injective homomorphism $\mathrm{Gal}(L|\mathbb{Q}) \hookrightarrow H$, where L is a finite Galois extension of $\mathbb{Q}$.

The only bad prime for the covering ϕ is $p = 2$. Let $\mathcal{S} = \{2\}$, and $R = \mathbb{Z}[\mathcal{S}^{-1}] = \mathbb{Z}[1/2]$. So, we are really interested in the subgroup $\mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, G) \subset \mathrm{H}^1(\mathbb{Q}, G)$ corresponding to those injective homomorphisms $\rho\colon\ \mathrm{Gal}(L|\mathbb{Q}) \hookrightarrow G$ for which L is possibly ramified only above $p = 2$. The possible fields are

$$L \in \left\{\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\zeta_8)\right\}.$$

Descent theory tells us that the set $\Omega_{\mathcal{S}}(2,2,2) := \mathbb{P}^1(2,2,2)\langle R\rangle \cong [\mathbb{P}^1_R/\operatorname{Aut}(\Phi)]\langle R\rangle$ is partitioned by the disjoint union of the sets $\phi_\rho(Z_\rho(\mathbb{Q}))$, as ρ ranges over $\mathrm{H}^1_{\mathcal{T}}(\mathbb{Q}, G)$. This already implies that

$$N(\Omega_{\mathcal{S}}(2,2,2); h) = \sum_{\rho} N(\phi_\rho(Z_\rho(\mathbb{Q})); h) \sim \kappa((2,2,2), \mathcal{S}) \cdot h^{1/2},$$

for some explicitly computable constant $\kappa((2,2,2), \mathcal{S}) > 0$.

Step 3: We will show that the count above already contains the counts $N(\Omega(2,2,2); h)$ and $N(\Omega(F_3); h)$ that we seek. Indeed, starting from the partition

$$\mathbb{P}^1(2,2,2)\langle R\rangle = \bigsqcup_{\rho \in \mathrm{H}^1_{\mathcal{T}}(\mathbb{Q}, G)} \phi_\rho(Z_\rho(\mathbb{Q})),$$

we note that by properties of Belyi maps, we can assigny to each $\rho \in \mathrm{H}^1_{\mathcal{T}}(\mathbb{Q}, G)$ a unique 2-simplified coefficient (A_ρ, B_ρ, C_ρ) such that $\phi_\rho(Z_\rho(\mathbb{Q}))$ is contained in the set

$$\Omega(A_\rho \mathsf{x}^2 + B_\rho \mathsf{y}^2 + C_\rho \mathsf{z}^2 = 0).$$

In particular, since $\Omega(F_1) \subset \Omega(2,2,2) \subset \Omega_{\mathcal{S}}(2,2,2)$, we deduce that

$$\Omega(F_3) \approx \bigsqcup_{\substack{\rho \in \mathrm{H}^1_{\mathcal{T}}(\mathbb{Q},G) \\ j(\mathcal{U}_3(\mathbb{Z})) \cap \phi_\rho(\mathbb{P}^1(\mathbb{Q})) \neq \varnothing}} \phi_\rho(Z_\rho(\mathbb{Q})),$$

where the $\approx$ sign denotes that the difference of the two sets is contained in $\{0, 1, \infty\}$. Combining this with Lehmer's count of primitive integral solutions to the Pythagorean equation, we conclude that

$$N(\Omega(F_1); h) = N(\Omega(F_2); h) = N(\Omega(F_3); h) \sim \tfrac{8}{\pi} \cdot h^{1/2}.$$

□

The set $\Omega(a, b, c)$ and the primitive integral solutions to the equation are closely related when $A, B, C \in \mathbb{Z}^\times = \{\pm 1\}$. Indeed, given $Q \in \Omega(a, b, c)$, then $|\operatorname{num}(Q)| = |x|^a$, $|\operatorname{num}(Q-1)| = |y|^b$ and $|\operatorname{den}(Q)| = |z|^c$. From the identity

$$-\operatorname{num}(Q) + \operatorname{num}(Q-1) + \operatorname{den}(Q) = 0,$$

we deduce that (x, y, z) is a primitive integral solution to Equation (1.1) for some choice of $(A, B, C) \in \{\pm 1\}^3 / \{\pm 1\}$. Conversely, given a primitive integral solution (x, y, z) to the equations

$$\mathsf{x}^a + \mathsf{y}^b + \mathsf{z}^c = 0, \quad \mathsf{x}^a + \mathsf{y}^b - \mathsf{z}^c = 0, \quad \mathsf{x}^a - \mathsf{y}^b + \mathsf{z}^c = 0, \quad \mathsf{x}^a - \mathsf{y}^b - \mathsf{z}^c = 0,$$

we see that $Q = -x^a/z^c$ is in $\Omega(a, b, c)$. By carefully identifying how the sets $\Omega(F)$

partition $\Omega(a,b,c)$ (or rather, certain supersets $\Omega_{\mathcal{S}}(a,b,c) \supset \Omega(a,b,c)$) we are able to obtain the following (stronger) result.

Theorem 1.2.0.d. *Consider Equation* (1.1) *with* $A, B, C \in \mathbb{Z}^3$ *nonzero and* $a, b, c > 1$. *Suppose that* $\chi := \chi(a,b,c) > 0$, *and that there exists at least one primitive integral solution to* F. *Then, there exists an explicit constant* $\kappa(F) > 0$ *such that for every* $\varepsilon > 0$,

$$N(\Omega(F), h) = \kappa(F) \cdot h^{\chi} + O(h^{\chi/2+\varepsilon}),$$

as $h \to \infty$. *The implied constant depends on* F *and* ε.

Chapter 2

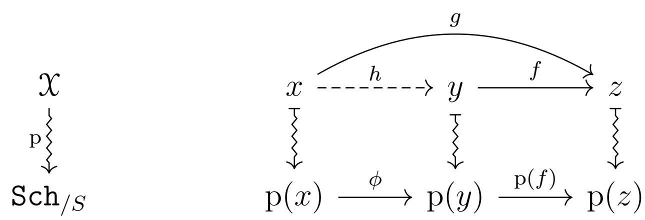
Background

We are interested in the arithmetic of certain stacks that arise in the study of generalized Fermat equations. In this chapter, we recall the definition of the functor of points of a stack and elaborate on the two examples most relevant to our context: quotient stacks and root stacks.

2.1 The groupoid of points on a stack

Recall that a morphism of schemes is fppf if it is faithfully flat and locally of finite presentation (see [28, Definition 3.4.1]). For a choice of base scheme S, we work on the big fppf site $S_{\mathtt{fppf}} = (\mathtt{Sch}_{/S})_{\mathtt{fppf}}$. This is the category $\mathtt{Sch}_{/S}$ of schemes over S where the open coverings are families $\{U_i \to U\}$ of S-morphisms such that $\bigsqcup_i U_i \to U$ is fppf.

Definition 2.1.0.a. A category over S is a pair $(\mathcal{X}, \mathrm{p})$ where $\mathcal{X}$ is a category and $\mathrm{p}\colon \mathcal{X} \rightsquigarrow \mathtt{Sch}_{/S}$ is a functor. A morphism $f\colon y \to z$ in $\mathcal{X}$ is called cartesian if given any morphism $g\colon x \to z$ and a factorization $\mathrm{p}(f) \circ \phi\colon \mathrm{p}(x) \to \mathrm{p}(y) \to \mathrm{p}(z)$ of $\mathrm{p}(g)$, there exists a unique morphism $h\colon x \to y$ such that $\mathrm{p}(h) = \phi$ and $g = h \circ f$.



(2.1)

Definition 2.1.0.b. Let $(\mathcal{X}, \mathrm{p})$ be a category over S. If $f: y \to z$ is a cartesian morphism, the object $y \in \mathcal{X}$ is called a pullback of z along $\mathrm{p}(f)$. Given an S-scheme U, the category of U-points in $\mathcal{X}$, denoted $\mathcal{X}(U)$, is the category of pullbacks over the identity. That is,

Objects: objects u in $\mathcal{X}$ such that $\mathrm{p}(u) = U$.

Morphisms: morphisms $\phi: v \to u$ in $\mathcal{X}$ such that $\mathrm{p}(\phi) = \mathrm{id}_U$.

Definition 2.1.0.c. A fibered category over S is a category $(\mathcal{X}, \mathrm{p})$ over S such that for every S-morphism of schemes $\Phi: V \to U$ and u in $\mathcal{X}(U)$, there exists a cartesian morphism $\phi: v \to u$ such that $\mathrm{p}(\phi) = \Phi$. In particular, this implies that v is in $\mathcal{X}(V)$.

Fibered categories over S assemble into a 2-category (see [25, Definition 3.1.3]). Indeed, there are natural notions of (i) morphisms between fibered categories over S, and (ii) morphisms between morphisms of fibered categories over S. Moreover, there is a version of the Yoneda lemma (see [25, Chapter 3.2]) in this context that justifies calling $U \mapsto \mathcal{X}(U)$ a "functor" of points.

Definition 2.1.0.d. Recall that a groupoid is a category in which every morphism is an isomorphism. A category fibered in groupoids over S if a fibered category $\mathcal{X}$ over S, such that for every S-scheme U, the category $\mathcal{X}(U)$ is a groupoid. Given a category fibered in groupoids $\mathcal{X}$ over S and an S-scheme U, we denote by $\mathcal{X}\langle U \rangle$ the set of isomorphism classes of the groupoid $\mathcal{X}(U)$.

Since our focus will be on the arithmetic of stacks, thinking about stacks in terms of their groupoids/sets of U-points will be enough for most of our applications. When we use the word *stack*, we mean an algebraic stack in the following sense.

Definition 2.1.0.e. Let $\mathcal{X}$ be a category fibered in groupoids over S.

(i) $\mathcal{X}$ is a stack if for every fppf cover $\{U_i \to U\}$, the induced descent functor $\mathcal{X}(U) \to \mathcal{X}(\{U_i \to U\})$ is an equivalence of categories. See [25, Section 4.2.4].

(ii) A stack $\mathcal{X}$ is algebraic if the diagonal $\Delta\colon \mathcal{X} \to \mathcal{X} \times_S \mathcal{X}$ is representable by an algebraic space, and $\mathcal{X}$ admits a smooth surjection $X' \to \mathcal{X}$ from an S-scheme X'. The map $X' \to \mathcal{X}$ is called a smooth presentation of $\mathcal{X}$. See [25, Section 8.1].

(iii) An algebraic stack $\mathcal{X}$ is Deligne–Mumford if the smooth presentation above is in fact étale. See [25, Section 8.3].

2.2 H^1, torsors, and quotient stacks

2.2.1 Nonabelian Čech cohomology

We follow [23, pp. 122] with the notations of [28, Section 6.4.4]. Let $\mathcal{G}$ be a sheaf of groups on a site $\mathcal{S}$, written multiplicatively. We allow the possibility that $\mathcal{G}$ is not abelian. Let $\mathcal{U} = \{U_i \to U\}_{i\in I}$ be a covering. A 1-cocycle for $\mathcal{U}$ with values in $\mathcal{G}$ is a family $g = \{g_{ij} \in \mathcal{G}(U_{ij}) : (i,j) \in I \times I\}$ such that:

$$(g_{ij}|_{U_{ijk}})(g_{jk}|_{U_{ijk}}) = g_{ik}|_{U_{ijk}} \quad \text{for all } (i,j,k) \in I \times I \times I.$$

Two 1-cocycles g, g' for $\mathcal{U}$ with values in $\mathcal{G}$ are said to be cohomologous if there is a family $h = \{(h_i) \in \mathcal{G}(U_i) : i \in I\}$, such that:

$$g'_{ij} = (h_i|_{U_{ij}})g_{ij}(h_j|_{U_{ij}})^{-1}, \qquad \text{for all } (i,j) \in I \times I.$$

This is an equivalence relation, and we denote by $\check{\mathrm{H}}^1(\mathcal{U}, \mathcal{G})$ the set of equivalence classes. Note that this set has a distinguished element, namely the class of the family of identities $\{1 \in \mathcal{G}(U_{ij}) : (i,j) \in I \times I\}$. We define the Čech cohomology set $\check{\mathrm{H}}^1(U, \mathcal{G})$

to be the direct limit of the pointed sets $\check{\mathrm{H}}(\mathcal{U}, \mathcal{G})$, where the direct limit is taken over all open coverings $\mathcal{U}$ of U ordered by refinement.

Proposition 2.2.1.a. *To any short exact sequence of sheaves of groups on a site $\mathcal{S}$, and any object U in $\mathcal{S}$*

$$1 \longrightarrow \mathcal{G}' \to \mathcal{G} \to \mathcal{G}'' \to 1,$$

there is an exact sequence of pointed sets

$$1 \longrightarrow \mathcal{G}'(U) \to \mathcal{G}(U) \to \mathcal{G}''(U) \xrightarrow{\delta} \check{\mathrm{H}}^1(U, \mathcal{G}') \to \check{\mathrm{H}}^1(U, \mathcal{G}) \to \check{\mathrm{H}}^1(U, \mathcal{G}'').$$

2.2.2 Torsor sheaves

We follow [25, Section 4.5], [28, Section 6.5.4], and [23, Section III.4].

Let $\mathcal{S}$ be a site, and let $\mathcal{G}$ be a sheaf of groups on $\mathcal{S}$.

Definition 2.2.2.a (Torsor sheaves)**.** A right $\mathcal{G}$-torsor on $\mathcal{S}$ is a sheaf of sets $\mathcal{Z}$ together with a right action $\rho\colon \mathcal{Z} \times \mathcal{G} \to \mathcal{Z}$ such that the following conditions hold:

1. For every $U \in \mathcal{S}$, there exists a covering $\{U_i \to U\}_{i \in I}$ such that $\mathcal{Z}(U_i) \neq \varnothing$ for all $i \in I$.
2. The map $\mathcal{Z} \times \mathcal{G} \to \mathcal{Z} \times \mathcal{Z}$ defined by $(x, g) \mapsto (x, x \cdot g)$ is an isomorphism.

A morphism of $\mathcal{G}$-torsors $(\mathcal{Z}_1, \rho_1) \to (\mathcal{Z}_2, \rho_2)$ is a morphism of sheaves $f\colon \mathcal{Z}_1 \to \mathcal{Z}_2$ such that the following square commutes.

$$\begin{array}{ccc} \mathcal{Z}_1 \times \mathcal{G} & \xrightarrow{f \times \mathrm{id}_{\mathcal{G}}} & \mathcal{Z}_2 \times \mathcal{G} \\ {\scriptstyle \rho_1}\downarrow & & \downarrow{\scriptstyle \rho_2} \\ \mathcal{Z}_1 & \xrightarrow[f]{} & \mathcal{Z}_2 \end{array}$$

A silly yet important example is the trivial $\mathcal{G}$-torsor. This is the sheaf $\mathcal{G}$ itself, equipped with the right $\mathcal{G}$-action given by the multiplication law. Note that Item 1 in Definition 2.2.2.a is satisfied, since for every U in $\mathcal{S}$, the group $\mathcal{G}(U)$ contains the identity element. We say that an open cover $\{U_i \to U\}_{i\in I}$ trivializes $\mathcal{Z}$ if there exist isomorphisms $f_i \colon \mathcal{Z}|_{U_i} \to \mathcal{G}|_{U_i}$ of $\mathcal{G}|_{U_i}$-torsors for every $i \in I$. We could have defined sheaf torsors as sheaves of sets with a group action admitting a trivializing cover (see [28, Definition 6.5.7]).

Proposition 2.2.2.b. *Let $\mathcal{G}$ be a group sheaf on a site with final object S. Then, there is an isomorphism of pointed sets*

$$\frac{\{\mathcal{G}\text{-}\textit{torsor sheaves}\}}{\textit{isomorphism}} \to \check{\mathrm{H}}^1(S, \mathcal{G}). \tag{2.2}$$

Proof. Let $\mathcal{Z}$ be a right $\mathcal{G}$-torsor sheaf. Choose a trivializing open cover $\mathcal{U} = \{U_i \to S\}$ with isomorphisms $f_i \colon \mathcal{G}|_{U_i} \to \mathcal{Z}|_{U_i}$. Then, on the overlaps $U_{ij} := U_i \times_S U_j$, the transition maps $f_i^{-1} \circ f_j \colon \mathcal{G}|_{U_{ij}} \xrightarrow{\sim} \mathcal{G}|_{U_{ij}}$ are given by left multiplication by some $g_{ij} \in \mathcal{G}(U_{ij})$. Since $(f_i^{-1} \circ f_j) \circ (f_j^{-1} \circ f_k) = f_i^{-1} \circ f_k$ when restricted to U_{ijk}, the family $g = \{g_{ij}\}$ obtained in this way is a 1-cocycle for $\mathcal{U}$. Furthermore, a different choice of isomorphisms $f_i' \colon \mathcal{G}|_{U_i} \to \mathcal{Z}|_{U_i}$ yields a cohomologous 1-cocycle g'. Indeed, the isomorphism $f_i^{-1} \circ f_i' \colon \mathcal{G}|_{U_i} \to \mathcal{G}|_{U_i}$ is given by left multiplication by an element $h_i \in \mathcal{G}(U_i)$. The family $h = \{h_i\}$ defined in this way witnesses the equivalence between g and g'. In this way, we get an isomorphism of sets

$$\frac{\{\mathcal{G}\text{-torsor sheaves trivialized by } \mathcal{U}\}}{\text{isomorphism}} \to \check{\mathrm{H}}^1(\mathcal{U}, \mathcal{G}).$$

Moreover, the isomorphism class of the trivial torsor is sent to the class of the trivial 1-cocycle. Taking the direct limit over all open coverings gives the desired isomorphism.

□

2.2.3 Torsor schemes

We follow [28, Section 6.5].

We narrow our focus to $\mathcal{S} = S_{\mathtt{fppf}}$ the fppf site over a base scheme S.

A torsor scheme is a representable torsor sheaf on $S_{\mathtt{fppf}}$. We will work with the following equivalent definition.

Definition 2.2.3.a (Torsor scheme)**.** Let $G \to S$ be an fppf group 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.

As before, a silly but important example is the trivial G-torsor. This is the fppf scheme $G \to S$ itself, with the right G-action given by the multiplication law. Observe that if $T \to S$ is a G-torsor, and $S' \to S$ is an fppf cover, then the base change $T' \to S'$ is a G'-torsor.

Lemma 2.2.3.b. *Let $T \to S$ be an S-scheme, equipped with a G-action $T \times_S G \to T$ satisfying Item 2 in Definition 2.2.3.a. The following conditions are equivalent.*

(a) $T \to S$ is fppf.

(b) $T \to S$ is fppf locally isomorphic to the trivial G-torsor.

(c) $T \to S$ admits a section fppf locally.

Proof.

(a) $\Leftrightarrow$ (b). Assume (a), and let ϕ be the isomorphism $T \times_S G \to T \times_S T$. Then ϕ is the pullback of $G \to S$ by the fppf cover $\pi\colon T \to S$. In other words, $T_T \cong G_T$ as

T-schemes. Furthermore, the G_T-actions coincide: this is the formula $(xg)h = x(gh)$ coming from the definition of a right action. Thus $T_T \cong G_T$ as G_T-torsors. Conversely, assume (b). There exists an fppf cover $S' \to S$ such that $T' \cong G'$ as G'-torsors over S'. Since $G' \to S'$ is fppf, so is $\pi' \colon T' \to S'$. By fpqc descent [28, Theorem 4.3.7], the original map $\pi \colon T \to S$ is also fppf.

(b) $\Leftrightarrow$ (c). Assume (b) and let $S' \to S$ be a trivializing fppf cover. Since $G' \to S'$ has a section (the identity) so does $\pi' \colon T' \to S'$. Conversely, assume (c) and let $S' \to S$ be an fppf cover over which π admits a section $\sigma \colon S' \to T'$.

$$\begin{array}{ccc} T' & \longrightarrow & T \\ {\scriptstyle \sigma}\curvearrowright\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ S' & \longrightarrow & S \end{array}$$

Using the same argument as above, we know that $T'_{T'} \cong G'_{T'} \cong G_{T'}$ as $G_{T'}$-torsors over T'. Base changing this isomorphism by σ, we get that T' and G' are isomorphic as G'-torsors over S', as we wanted to show. □

We have seen in Proposition 2.2.2.b that $\check{\mathrm{H}}^1(S, G)$ is in bijective correspondence with isomorphism classes of torsor sheaves on $S_{\mathtt{fppf}}$. In many cases of interest, isomorphism classes of torsor sheaves coincide with isomorphism classes of torsor schemes.

Theorem 2.2.3.c ([28, Theorem 6.5.10]). *Let G be an fppf group scheme over a locally noetherian scheme S. Then, we have*

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

Moreover, the first injection is a bijection in any of the following cases:

(i) $G \to S$ is an affine morphism.

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

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

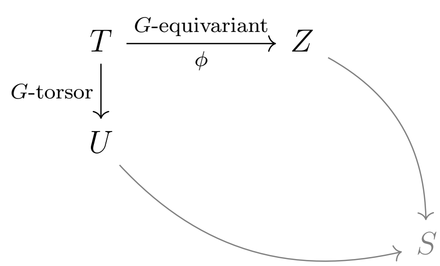
2.2.4 Quotient stacks

Situation 2.2.4.a. Here

- S is a scheme.
- Z is a scheme over S.
- G is an fppf S-group scheme.
- $Z \times_S G \to Z$ is a right action of G, defined over S.
- We abbreviate $\mathrm{H}^1 = \check{\mathrm{H}}^1_{\mathtt{fppf}}$, as in Section 2.2.1.

Definition 2.2.4.b (Quotient stack)**.** Assume we are in Situation 2.2.4.a. Define the quotient stack of Z by G, denoted $[Z/G]$, to be the stack over $S_{\mathtt{fppf}}$ with:

Objects: triples (U, T, ϕ)



where

(i) U is an S-scheme,

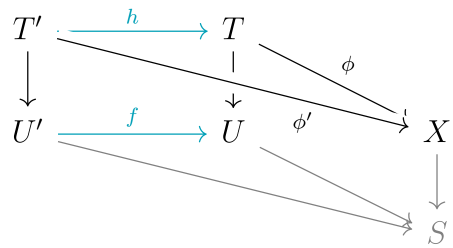
(ii) $T \to U$ is a right fppf G_U-torsor, and

(iii) $\phi\colon T \to Z$ is a G-equivariant S-morphism.

Morphisms: $(U', T', \phi') \to (U, T, \phi)$ are pairs (f, h), where

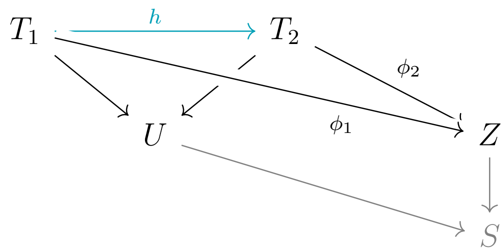
(iv) $f\colon U' \to U$ is an S-morphism of schemes, and

(v) $h\colon T' \to T$ is a G-equivariant morphism over f inducing an isomorphism of $G_{U'}$-torsors $T' \cong T \times_{f,U} U'$, such that $\phi' = \phi \circ h$.



(2.3)

In particular, for any given S-scheme U, the groupoid $[Z/G](U)$ consists of pairs (T, ϕ) with $T \to U$ a G_U-torsor, and $\phi\colon T \to Z$ a G-equivariant S-morphism; and isomorphisms $h\colon (T_1, \phi_1) \to (T_2, \phi_2)$ are simply isomorphisms $h\colon T_1 \to T_2$ of G_U-torsors, compatible with the maps to Z.



(2.4)

The following lemma is [25, Exercise 10F].

Lemma 2.2.4.c (Induced maps on quotient stacks)**.** *Let S be a scheme, and $\varphi\colon G \to H$ a homomorphism of fppf group schemes over S. Let X be an S-scheme with a right G-action, and Y and S-scheme with a right H-action. Suppose that there is an S-morphism $f\colon X \to Y$ that is compatible with the group actions. Then, f induces a morphism of algebraic stacks $\bar{f}\colon [X/G] \to [Y/H]$.*

2.2.5 The method of descent

In this section, we summarize the basics of descent theory. We follow Skorobogatov's book [34, pp. 20], but with inverted handedness. We recast the geometric operations on torsors from the point of view of quotient stacks.

Situation 2.2.5.a. We are in Situation 2.2.4.a. Furthermore, we will restrict to the the case where:

- Z is quasi-projective.
- T denotes a **left** fppf G-torsor over S.
- $[Z/G]$ is the quotient stack, and $f\colon Z \to [Z/G]$ is the projection map. We emphasize that $[Z/G]$ need not be a scheme.
- $G \to S$ is affine. This assumption is not necessary, but it will ensure that $\mathrm{H}^1(S, G)$ is in bijection with isomorphism classes of G-torsor schemes, as a consequence of Theorem 2.2.3.c.

The main definition of this section is the following.

Definition 2.2.5.b (Contracted product)**.** The contracted product $Z \overset{G}{\times} T$ is defined as the quotient stack $[Z \times_S T/G]$, where G acts on the **right** on $Z \times_S T$ via

$$(z, t) \cdot g := (z \cdot g, g^{-1} \cdot t).$$

The following lemma is a restatement of [28, Section 6.5.6].

Lemma 2.2.5.c (Twisting by fppf descent)**.** *Suppose we are in Situation 2.2.5.a. Given $\tau \in \mathrm{H}^1(S, G)$, let $T \to S$ be a **left** fppf G-torsor corresponding to τ. Then:*

(i) The contracted product $Z \overset{G}{\times} T$ is an affine fppf S-scheme. We call this the twist of Z by τ, and denote it Z_τ. There is an induced map $f_\tau\colon Z_\tau \to [Z/G]$, called the twist of f by τ.

(ii) If $T = G$ is the trivial left G-torsor, then $Z_\tau \cong Z$ as S-schemes with a right G-action.

(iii) Taking $Z = G$ acting on itself by conjugation, the twist $Z_\tau = G_\tau$ is an affine fppf group scheme over S. It is called the ***inner twist*** *of G by τ.*

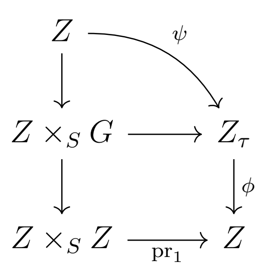
(iv) The twist Z_τ is a right fppf G_τ-torsor over S. Moreover, there is an isomorphism $[Z/G] \cong [Z_\tau/G_\tau]$.

(v) T is a (G, G_τ)-bitorsor. The same S-scheme T is a (G_τ, G)-bitorsor, which we call the ***inverse torsor*** *T^{-1}.*

(vi) $T^{-1} \overset{G}{\times} T$ is isomorphic to the trivial G-torsor.

Proof. (i) The representability of $Z_\tau = Z \overset{G}{\times} T$ is [34, Lemma 2.2.3]. The fact that $T \to S$ is affine follows from the affineness of $G \to S$. For the second statement, note that we have a G-equivariant morphism $Z \times_S T \to Z$, namely the first projection $(z, t) \mapsto z$. From Lemma 2.2.4.c, we get that $f_\tau \colon [Z \times_S T/G] \to [Z/G]$ is the induced map of quotient stacks.

(ii) We have the morphism $Z \times_S G \to Z \times_S Z$ given by $(z, g) \mapsto (z, z \cdot g)$. Observe that it is G-equivariant for the twisted action on $Z \times_S G$, and the action $(z_1, z_2) \cdot g := (z_1 \cdot g, z_2)$ on $Z \times_S Z$. This gives a morphism of quotient stacks $\psi \colon Z_\tau \to Z$. On the other hand, we have a morphism $Z \to Z_\tau$ induced by $\phi \colon Z \to Z \times_S G$. To see that these are mutual inverses, it is enough to realize that the following diagram is commutative.



(iii) We already verified the affineness claim. The rest is a matter of pulling back the group operations to T and verifying that they are G-equivariant under the twisted action. For example, consider the inverse morphism $\iota \colon G \to G$ pulled back to $\iota \times_S T \colon G \times_S T \to G \times_S T$. Then, we have that $(g, t) \cdot h = (h^{-1}gh, h^{-1}t)$ maps to

$(h^{-1}g^{-1}h, h^{-1}t) = (g^{-1}, t) \cdot h$. We obtain the twisted inverse morphism $G_\tau \to G_\tau$ by passing to the quotient.

(iv) Consider the morphism $\phi\colon (Z \times_S T) \times_S (G \times_S T) \to Z \times_S T$ given on points by $(z, x, g, t) \mapsto (z \cdot g, t)$. Note that $(z, x, g, t) \cdot h = (z \cdot h, h^{-1}x, h^{-1}gh, h^{-1}t)$ maps to $(z \cdot gh, h^{-1}t) = (z \cdot g, t) \cdot h$, so ϕ induces a morphism $Z_\tau \times_S G_\tau \to Z_\tau$. One similarly verifies the G-equivariance of the diagrams that descend to the group action axioms on $Z_\tau \times_S G_\tau \to Z_\tau$.

(v) Follows directly from (iv).

(vi) This is a particular instance of the general fact that $Z \times_{[Z/G]} Z \cong Z \times_S G$. Indeed, taking $Z = T^{-1} \times_S T$ shows that Z_τ has a section fppf locally, implying that it is the trivial G-torsor by Lemma 2.2.3.b. □

Theorem 2.2.5.d (The method of descent)**.** *Suppose we are in Situation 2.2.5.a. Then, the* ***set*** *of S-points on the quotient stack $[Z/G]$ is partitioned by the images of the S-points of the twists of $f\colon Z \to [Z/G]$.*

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

Proof. Recall that a map $S \to [Z/G]$ is the data of a pair (T^{-1}, ϕ) where T^{-1} is a right fppf G-torsor over S, and $\phi\colon T^{-1} \to Z$ is a G-equivariant map of S-schemes. We want to show that every map $(T^{-1}, \phi)\colon S \to [Z/G]$ factors through a twist $f_\tau\colon Z_\tau \to [Z/G]$ of the canonical quotient $f\colon Z \to [Z/G]$, where τ is completely determined by the isomorphism class of the point (T, ϕ). Indeed, in this setting, we have the *evaluation map* $\zeta\colon (T^{-1}, \phi) \mapsto \tau := [T \to S]$ from $[Z/G]\langle S\rangle$ to $\mathrm{H}^1(S, G)$, where τ is the cohomology class corresponding to the left G-torsor $T \to S$ via Theorem 2.2.3.c. Since $T^{-1} \overset{G}{\times} T$ is isomorphic to the trivial G-torsor, we have a section $e\colon S \to T^{-1} \overset{G}{\times} T$ that realizes the factorization of our map (T^{-1}, ϕ) by the commutativity of the diagram in Figure 2.1. The map $T^{-1} \overset{G}{\times} T \to Z_\tau$ is the one induced by the G-equivariant

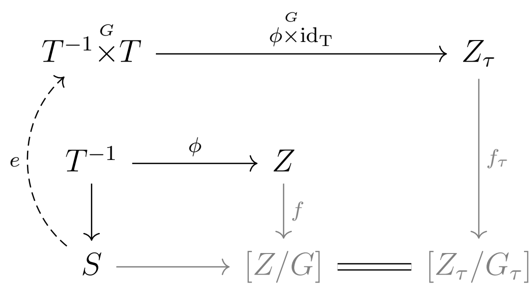


Figure 2.1: Proof of the method of descent.

S-morphism $\phi \times_S \mathrm{id}_T \colon T^{-1} \times_S T \to Z \times_S T$. □

2.3 The root stack construction

2.3.1 Generalized effective Cartier divisors

Recall that an effective Cartier divisor on a scheme X is a closed subscheme $D \subset X$ such that the corresponding ideal sheaf $\mathcal{O}_X(-D)$ is a line bundle [35, Tag 01WR]. Equivalently, a closed subscheme is an effective Cartier divisor if and only if it is locally cut out by a single element which is a nonzero divisor [35, Tag 01WS]. Denote by $j_D \colon \mathcal{O}_X(-D) \hookrightarrow \mathcal{O}_X$ the natural inclusion morphism of $\mathcal{O}_X$-modules.

Definition 2.3.1.a ([25, Definition 10.3.2])**.** A generalized effective Cartier divisor on a scheme X is a pair $(\mathcal{L}, \rho)$, where $\mathcal{L}$ is a line bundle on X, and $\rho \colon \mathcal{L} \to \mathcal{O}_X$ is a morphism of $\mathcal{O}_X$-modules. An isomorphism between generalized Cartier divisors $(\mathcal{L}', \rho') \cong (\mathcal{L}, \rho)$ is an isomorphism of line bundles $\sigma \colon \mathcal{L}' \to \mathcal{L}$ such that the following triangle commutes

$$\begin{array}{ccc} \mathcal{L}' & \xrightarrow{\sigma} & \mathcal{L} \\ & {\scriptstyle \rho'} \searrow \quad \swarrow {\scriptstyle \rho} & \\ & \mathcal{O}_X & \end{array} .$$

We can multiply generalized effective Cartier divisors $(\mathcal{L}, \rho)$ and $(\mathcal{L}', \rho')$ by declaring $(\mathcal{L}, \rho) \cdot (\mathcal{L}', \rho') := (\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}', \rho \otimes \rho')$, where $\rho \otimes \rho'$ is the morphism of $\mathcal{O}_X$-modules given by the composition $\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}' \to \mathcal{O}_X \otimes_{\mathcal{O}_X} \mathcal{O}_X \cong \mathcal{O}_X$.

Example 2.3.1.b. Given an effective Cartier divisor $D \subset X$, the pair $(\mathcal{O}_X(-D), j_D)$ is a generalized effective Cartier divisor. By definition, two effective Cartier divisors $D', D \subset X$ are isomorphic as generalized effective Cartier divisors if and only if they are equal and the isomorphism is therefore unique.

Example 2.3.1.c (Generalized effective Cartier divisors on affine schemes)**.** In light of the equivalence between R-modules and quasicoherent $\mathcal{O}_X$-modules on $X = \operatorname{Spec} R$, a generalized effective Cartier divisor on an affine scheme is of the from $(\widetilde{M}, \widetilde{\lambda})$ for a projective R-module M of rank one, and a morphism $\lambda\colon M \to R$ of R-modules. In particular, $\lambda(M)$ is an ideal in R. Two generalized effective Cartier divisors (M', λ') and (M, λ) on $\operatorname{Spec} R$ are isomorphic if and only if there exists an R-module isomorphism $\sigma\colon M' \to M$ such that $\lambda' = \lambda \circ \sigma$. In particular, note that such a pair gives rise to the same ideal $\lambda'(M') = \lambda(\sigma(M')) = \lambda(M)$.

2.3.2 Definition of a root stack

Definition 2.3.2.a (Root stack)**.** Fix a generalized effective Cartier divisor $(\mathcal{L}, \rho)$ on a scheme X, and a positive integer r. Let $\sqrt[r]{X; (\mathcal{L}, \rho)}$ be the fibered category over the category $\mathtt{Sch}_{/X}$ with:

Objects: triples $(f\colon T \to X, (\mathcal{M}, \lambda), \sigma)$ where $f\colon T \to X$ is an X-scheme, $(\mathcal{M}, \lambda)$ is a generalized effective Cartier divisor on T, and $\sigma\colon (\mathcal{M}^{\otimes r}, \lambda^{\otimes r}) \to (f^*\mathcal{L}, f^*\rho)$ is an isomorphism of generalized effective Cartier divisors on T.

Morphisms: a morphism $(f'\colon T' \to X, (\mathcal{M}', \lambda'), \sigma') \to (f\colon T \to X, (\mathcal{M}, \lambda), \sigma)$ is the data of a pair $(h, h^\flat)$ where $h\colon T' \to T$ is an X-morphism, and $h^\flat\colon (\mathcal{M}', \lambda') \to (h^*\mathcal{M}, h^*\lambda)$ is an isomorphism of generalized effective Cartier divisors on T' such that the following diagram commutes

$$\begin{array}{ccc} \mathcal{M}'^{\otimes r} & \xrightarrow{h^{\flat \otimes r}} & h^*\mathcal{M}^{\otimes r} \\ {\scriptstyle \sigma'}\downarrow & & \downarrow{\scriptstyle h^*\sigma} \\ (f')^*\mathcal{L} & \xrightarrow{\sim} & h^*f^*\mathcal{L}. \end{array}$$

Remark 2.3.2.b (Points on a root stack)**.** By Definition 2.3.2.a, $\mathcal{X}$ is defined over the base X, i.e., it is a fibered category over $\mathtt{Sch}_{/X}$. In particular, the notation $\mathcal{X}(\mathbb{Z})$ is abusive. To justify it, we consider $\mathcal{X}$ as a stack over $\operatorname{Spec}\mathbb{Z}$, composing with the forgetful map $\mathtt{Sch}_{/X} \to \mathtt{Sch}$. This allows us to consider the groupoid $\mathcal{X}(\mathbb{Z})$ as the disjoint union over $x \in X(\mathbb{Z})$ of the groupoids $\mathcal{X}(x\colon \operatorname{Spec}\mathbb{Z} \to X)$. More generally, when base changing to $S_{\mathtt{fppf}}$ for some base scheme S, the scheme $X \in \mathtt{Sch}_{/S}$, and the root stack $\mathcal{X}$ will be initially defined over $(S_{\mathtt{fppf}})_{/X}$. Our standing convention will be to denote by $\mathcal{X}(S)$ the disjoint union over $x \in \operatorname{Hom}_S(S, X) = X(S)$ of the groupoids $\mathcal{X}(x)$.

We are concerned with the special case in which we root a scheme at a good old Cartier divisor D. We abbreviate $\sqrt[r]{X; (\mathcal{O}_X(-D), j_D)}$ by $\sqrt[r]{X; D}$. In particular, given an X-scheme $f\colon T \to X$, the groupoid $\sqrt[r]{X; D}(f)$ consists of:

Objects: triples $(f\colon T \to X, (\mathcal{M}, \lambda), \sigma)$ where $(\mathcal{M}, \lambda)$ is a generalized effective Cartier divisor on T, and $\sigma\colon (\mathcal{M}^{\otimes r}, \lambda^{\otimes r}) \to (f^*\mathcal{O}_X(-D), f^*j_D)$ is an isomorphism of generalized effective Cartier divisors on T.

Isomorphisms: $(f\colon T \to X, (\mathcal{M}', \lambda'), \sigma') \to (f\colon T \to X, (\mathcal{M}, \lambda), \sigma)$ consist of pairs $(h, h^\flat)$ where $h \in \operatorname{Aut}(T)$ satisfies $f = f \circ h$, and $h^\flat\colon (\mathcal{M}', \lambda') \to (h^*\mathcal{M}, h^*\lambda)$ is an isomorphism of generalized effective Cartier divisors on T such that the following diagram commutes

$$\begin{array}{ccc} \mathcal{M}'^{\otimes r} & \xrightarrow{h^{\flat \otimes r}} & h^*\mathcal{M}^{\otimes r} \\ {\scriptstyle \sigma'}\downarrow & & \downarrow{\scriptstyle h^*\sigma} \\ (f)^*\mathcal{O}_X(-D) & \xrightarrow{\sim} & h^*f^*\mathcal{O}_X(-D). \end{array}$$

2.3.3 The projective line rooted at a point

Remark 2.3.3.a (PID points on the projective line)**.** Recall the greatest common divisor of two elements a, b in R is a generator of the ideal $aR + bR$. Let $\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$. We have that $\mathbb{P}^1(R) \cong \{(a,b) \in R^2 : aR + bR = R\} / R^\times$. One can see this using the fact that $\mathbb{P}^1$ is the quotient stack $[\mathcal{V}/\mathbb{G}_\mathrm{m}]$. Indeed, since $\operatorname{Pic} R$ is trivial, a point $Q \in \mathbb{P}^1(R)$ is (isomorphic to a) cartesian square

$$\begin{array}{ccc} \mathbb{G}_\mathrm{m} & \xrightarrow{\phi} & \mathcal{V} \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \longrightarrow & \mathbb{P}^1, \end{array}$$

where ϕ is a $\mathbb{G}_\mathrm{m}$-equivariant map. Composing the identity section $e\colon \operatorname{Spec} R \to \mathbb{G}_\mathrm{m}$ with ϕ we obtain a point in $\mathcal{V}(R)$, i.e., a pair $(a,b) \in R^2$ such that $aR + bR = R$. Any other isomorphic square comes from a $\mathbb{G}_\mathrm{m}$-equivariant map $\phi'\colon \mathbb{G}_\mathrm{m} \to \mathcal{V}$ giving rise to a point (a', b') such that $(a', b') = (ua, ub)$ for some $u \in R^\times$.

Definition 2.3.3.b. Let R be a principal ideal domain, and choose $P = (c : d)$ and $Q = (a : b)$ in $\mathbb{P}^1(R)$. Define the intersection ideal of P with Q as $I(P,Q) := (ad - bc)R \subset R$.

The ideal $I(P,Q)$ cuts out the locus in $\operatorname{Spec} R$ over which P and Q intersect. Indeed, the pullback of the diagonal $\mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1$ by $(P,Q)\colon \operatorname{Spec} R \to \mathbb{P}^1 \times \mathbb{P}^1$ gives the closed subscheme $\operatorname{Spec} R/I(P,Q)$. From the magic square, $I(P,Q)$ can equivalently be defined by the cartesian square

$$\begin{array}{ccc} \operatorname{Spec} R/I(P,Q) & \longrightarrow & \operatorname{Spec} R \\ \downarrow & & \big\downarrow{\scriptstyle Q} \\ \operatorname{Spec} R & \xhookrightarrow[P]{} & \mathbb{P}^1_R\,. \end{array} \tag{2.5}$$

Warning 2.3.3.c. The pullback $P^*\mathcal{O}_{\mathbb{P}^1}(-Q)$ does not coincide with $\widetilde{I(P,Q)}$. More generally, the pulback of a quasicoherent ideal sheaf need not coincide with the ideal sheaf of the pulled back closed subscheme (see [37, Remark 14.5.10]). Nevertheless, we have the following commutative diagram of sheaves on $\operatorname{Spec} R$ with exact rows

$$\begin{array}{ccccccccc} & & P^*\mathcal{O}_{\mathbb{P}^1}(-Q) & \longrightarrow & P^*\mathcal{O}_{\mathbb{P}^1} & \longrightarrow & P^*Q_*\widetilde{R} & \longrightarrow & 0 \\ & & \downarrow & \searrow^{\widetilde{\lambda}} & \| & & \| & & \\ 0 & \longrightarrow & \widetilde{I(P,Q)} & \longrightarrow & \widetilde{R} & \longrightarrow & \widetilde{R/I(P,Q)} & \longrightarrow & 0\,. \end{array} \tag{2.6}$$

Proposition 2.3.3.d. *Let R be a principal ideal domain with fraction field k. Let $\mathbb{P}^1 = \operatorname{Proj} R[\mathsf{s},\mathsf{t}]$. Fix a point $P \in \mathbb{P}^1(R)$, and a positive integer n. Let $\mathcal{X} := \sqrt[n]{\mathbb{P}^1; P}$ be the n^{th} root stack of $\mathbb{P}^1$ at P, defined over* $\operatorname{Spec} R$*. Then,*

$$\mathcal{X}(R) = \bigsqcup_{Q \in \mathbb{P}^1(R)} \mathcal{X}(Q),$$

where

(i) The fiber $\mathcal{X}(P)$ contains one object up to isomorphism, with automorphism group isomorphic to $\mu_n(R) = \{u \in R^\times : u^n = 1\}$.

(ii) For $Q \neq P$ the ideal $I(P,Q)$ is nonzero, and the fiber $\mathcal{X}(Q)$ contains one object with trivial automorphism group if and only if $I(P,Q) = J^n$ for some ideal $0 \neq J \subsetneq R$, and is empty otherwise.

In particular, when $R = k$, we have that $\mathcal{X}\langle k\rangle \cong \mathbb{P}^1(k)$.

Proof. Let $\mathcal{X} := \sqrt[n]{\mathbb{P}^1; P}$. As explained in Remark 2.3.2.b, the groupoid $\mathcal{X}(R)$ is the disjoint union of the groupoids $\mathcal{X}(Q)$, ranging over $Q \in \mathbb{P}^1(R)$. We proceed to describe each groupoid $\mathcal{X}(Q)$.

To start, consider the pullback of the ideal sheaf $\mathcal{O}_{\mathbb{P}^1}(-Q) = \widetilde{I_Q}$ via the map $P\colon \operatorname{Spec} R \to \mathbb{P}^1$, where $I_Q = (a\mathsf{t} - b\mathsf{s})R[\mathsf{s},\mathsf{t}] \subset R[\mathsf{s},\mathsf{t}]$. This is a line bundle on $\operatorname{Spec} R$ corresponding to a certain free R-module of rank one $M(P,Q)$. (Explicitly,

$M(P, Q)$ is the degree zero part of the tensor product of graded R-modules

$$(a\mathsf{t} - b\mathsf{s})R[\mathsf{s}, \mathsf{t}] \otimes_{R[\mathsf{s},\mathsf{t}]} \frac{R[\mathsf{s}, \mathsf{t}]}{(c\mathsf{t} - d\mathsf{s})R[\mathsf{s}, \mathsf{t}]},$$

but we will not use this description.) Moreover, the pullback of the generalized effective Cartier divisor $j_Q \colon \mathcal{O}_{\mathbb{P}^1}(-Q) \hookrightarrow \mathcal{O}^1_{\mathbb{P}}$ corresponds to an R-module homomorphism $\lambda(P, Q) \colon M(P, Q) \to R$ with image $I(P, Q)$, as illustrated in 2.6.

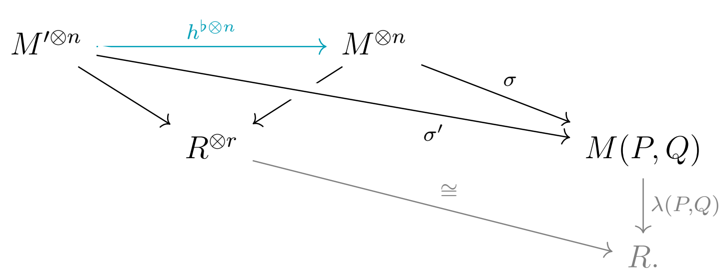
The **objects** in $\mathcal{X}(Q)$ are triples $(Q, (M, \lambda), \sigma)$, where

- (M, λ) is a generalized effective Cartier divisor on $\operatorname{Spec} R$ (see Example 2.3.1.c). Since R is a principal ideal domain, M is a free R-module of rank one and $\lambda \colon M \to R$ is an R-module homomorphism.
- $\sigma \colon (M^{\otimes n}, \lambda^{\otimes n}) \to (M(P, Q), \lambda(P, Q))$ is an isomorphism of generalized effective Cartier divisors on $\operatorname{Spec} R$, that is, a commutative triangle of R-modules

$$\begin{array}{ccc} M^{\otimes n} & \xrightarrow[\sigma]{\cong} & M(P,Q) \\ & {\scriptstyle \lambda^{\otimes n}} \searrow \quad \swarrow {\scriptstyle \lambda(P,Q)} & \\ & R. & \end{array} \tag{2.7}$$

By definition, an **isomorphism** $(Q, (M', \lambda'), \sigma') \to (Q, (M, \lambda), \sigma)$ in $\mathcal{X}(Q)$ is a pair $(h, h^\flat)$, where

- $h \colon \operatorname{Spec} R \to \operatorname{Spec} R$ is a morphism over $\operatorname{Spec} R$, so it must be the identity.
- $h^\flat \colon M' \to M$ is an isomorphism of R-modules such that $\lambda' = \lambda \circ h^\flat$ and the following diagram commutes



(2.8)

(i) When $P = Q$, then $I(P,Q) = 0$ and this forces every map $\lambda\colon M \to R$ to be the zero map. In particular, the bottom part of diagram (2.8) imposes no restriction and the isomorphisms of $\mathcal{X}(P)$ are precisely the isomorphisms of R-modules $h^\flat\colon M' \to M$ such that

$$\begin{array}{ccc} (M')^{\otimes n} & \xrightarrow[h^{\flat\otimes n}]{\cong} & M^{\otimes n} \\ & {\scriptstyle\sigma'}\searrow \quad \swarrow{\scriptstyle\sigma} & \\ & M(P,P). & \end{array}$$

In particular, any triple $(P,(M,\lambda),\sigma)$ in $\mathcal{X}(P)$ has $\mu_n(R)$ automorphisms.

(ii) When $P \neq Q$, the commutativity of (2.7) requires that the nonzero ideal $I(P,Q)$ is the n^{th} power of the ideal $\lambda(M)$ in R. This condition is also sufficient. Indeed, if $I(P,Q) = J^n$ for some nonzero ideal $\lambda\colon J \subset R$, then take an isomormphism of R-modules $\sigma\colon I(P,Q) \to M(P,Q)$ and note that

$$(Q,(J,\lambda),\sigma\colon J^n \to M(P,Q)) \tag{2.9}$$

is an object of $\mathcal{X}(Q)$, and every object in $\mathcal{X}(Q)$ is isomorphic to it. To calculate the automorphism group of this object, note that the only possible isomorphism $h^\flat\colon J \to J$ of R-modules such that $\lambda = h^\flat \circ \lambda\colon J \hookrightarrow R$, is the identity. Thus, the automorphism groups in $\mathcal{X}(Q)$ are trivial.

□

Chapter 3

Stacks associated to generalized Fermat equations

3.1 The projective line with three fractional points

3.1.1 A brief discussion of triangle groups

We collect a number of facts that we will use later. We follow [8, Section 2]. For more on this topic see [22, Chapter II].

Let $a, b, c > 1$ be positive integers. We say that the triple (a, b, c) is spherical, Euclidean, or hyperbolic according as the quantity

$$\chi(a,b,c) := \tfrac{1}{a} + \tfrac{1}{b} + \tfrac{1}{c} - 1$$

is positive, zero, or negative.

Definition 3.1.1.a. Given $a, b, c \in \mathbb{Z}_{\geqslant 2} \cup \{\infty\}$, the extended triangle group $\triangle(a, b, c)$ is defined as the group generated by elements $\delta_0, \delta_1, \delta_\infty, -1$, with -1 central in $\bar{\triangle}(a, b, c)$, subject to the relations $(-1)^2 = 1$ and

$$\delta_0^a = \delta_1^b = \delta_\infty^c = \delta_0\delta_1\delta_\infty = -1. \tag{3.1}$$

Define the triangle group $\bar{\triangle}(a, b, c)$ as the quotient of $\triangle(a, b, c)$ by $\{\pm 1\}$.

Let $\mathcal{H}(a, b, c)$ denote the simply connected Riemann surface with curvature corresponding to the sign of $\chi(a, b, c)$. Thus, $\mathcal{H}(a, b, c)$ is the Riemann sphere $\mathbb{CP}^1$ in the spherical case, the complex plane $\mathbb{C}$ in the euclidean case, and the upper-half plane $\mathcal{H}$ in the hyperbolic case. The reason to call them triangle groups is that they arise as groups of orientation-preserving isometries of a triangle with angles $\pi/a, \pi/b, \pi/c$ in the corresponding geometry $\mathcal{H}(a, b, c)$. Note that $\pi\chi(a, b, c)$ measures the difference between π and the sum of the angles of this triangle.

The spherical triangle groups are all finite groups. Moreover, they are all finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{Q}})$. These were classified by the German mathematician Felix Klein more than a century ago. By [8, Remark 2.2], we are safe to assume temporarily that the signature is nondecreasing: $a \leqslant b \leqslant c$.

- For the dihedral signatures $(a, b, c) = (2, 2, c)$ with $c \geqslant 2$, the triangle groups $\bar{\triangle}(2, 2, c)$ are isomorphic to the dihedral group D_c with $2c$ elements. In particular, $\bar{\triangle}(2, 2, 3)$ is isomorphic to the symmetric group in three letters S_3. The group $\bar{\triangle}(2, 2, 2)$ is isomorphic to the Klein four group $C_2 \times C_2$.

- For the tetrahedral signature $(a, b, c) = (2, 3, 3)$, the triangle group $\bar{\triangle}(2, 3, 3)$ is isomorphic to A_4; the group of rigid motions if the tetrahedron.

- For the octahedral signature $(a, b, c) = (2, 3, 4)$, the triangle group $\bar{\triangle}(2, 3, 4)$ is isomorphic to S_4; the group of rigid motions of the octahedron.

- For the icosahedral signature $(a, b, c) = (2, 3, 5)$, the triangle group $\bar{\triangle}(2, 3, 5)$ is isomorphic to A_5; the group of rigid motions of the icosahedron.

Table 3.1: Spherical triangle groups.

(a, b, c)	$\bar{\Delta}(a, b, c)$	$\chi(a, b, c)$
$(2, 2, c)$	D_c	$1/c$
$(2, 3, 3)$	A_4	$1/6$
$(2, 3, 4)$	S_4	$1/12$
$(2, 3, 5)$	A_5	$1/30$

3.1.2 Existence of Galois Belyi maps

Triangle groups arise as the monodromy groups of Galois Belyi maps.

Definition 3.1.2.a. Let Z be a nice[1] curve[2] defined over a field $k \subset \mathbb{C}$. A k-Belyi map is a finite k-morphism $\varphi\colon Z \to \mathbb{P}^1$ that is unramified outside $\{0, 1, \infty\}$.

These remarkable covers of the projective line are named after the Ukrainian mathematician G. V. Belyi , who famously proved that a complex algebraic curve can be defined over a number field if and only if it admits a $\mathbb{C}$-Belyi map [5, 6].

Definition 3.1.2.b. Let $\phi\colon Z_k \to \mathbb{P}^1_k$ be a k-Belyi map with automorphism k-group scheme $\operatorname{Aut}(\phi)$. We say that ϕ is geometrically Galois with Galois group G if the extension of function fields $\mathbf{k}(Z_{\bar{k}}) \supset \mathbf{k}(\mathbb{P}^1_{\bar{k}})$ is Galois, with Galois group G. Equivalently, ϕ is geometrically Galois if the monodromy group $\operatorname{Aut}(\phi_{\bar{k}})$ is isomorphic to G and acts transitively the fibers. This is the case if and only if $\#\operatorname{Aut}(\phi_{\bar{k}}) = \#G = \deg\phi$.

Remark 3.1.2.c. If $\phi\colon Z_k \to \mathbb{P}^1_k$ is a geometrically Galois k-Belyi map, for any $Q \in \mathbb{P}^1(k) - \{0, 1, \infty\}$, the fiber $\phi^{-1}(Q) := Z \times_k Q$ is a $\operatorname{Gal}(\phi)$-torsor over $\operatorname{Spec} k$.

Definition 3.1.2.d. 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

[1]Smooth, projective, geometrically integral.
[2]One dimensional separated scheme of finite type over a field.

critical value $P \in \{0, 1, \infty\}$. The Euler characteristic of φ is the quantity

$$\chi(\varphi) := \tfrac{1}{e_0} + \tfrac{1}{e_1} + \tfrac{1}{e_\infty} - 1. \tag{3.2}$$

As a consequence of the Riemann existence theorem, there exist Galois Belyi maps of any signature. See [13, Proposition 3.1] and [26, Lemma 2.5].

Proposition 3.1.2.e. *For any positive integers $a, b, c > 1$, there exists a number field K and a geometrically Galois K-Belyi map $\phi\colon Z_K \to \mathbb{P}^1_K$ of signature $(e_0, e_1, e_\infty) = (a, b, c)$. Let g be the genus of Z_K, and G be the monodromy group of ϕ. Then $2 - 2g = \deg \phi \cdot \chi(\phi)$. In particular,*

(i) If $\chi(\phi) > 0$, then $g = 0$ and $\deg \phi = \#G(\bar{K}) = 2/\chi(\phi)$.

(ii) If $\chi(\phi) = 0$, then $g = 1$.

(iii) If $\chi(\phi) < 0$, then $g > 1$.

A crucial fact that we will need later is that for each one of the spherical signatures, there exists a Galois Belyi defined over $\mathbb{Q}$. The maps presented in Table 3.1 are adapted from the parametrizations found in [9, Chapter 14]. The original sources can be found in [7] and [15].

Table 3.2: Examples of Galois $\mathbb{Q}$-Belyi maps for the spherical signatures.

(a, b, c)	$\bar{\triangle}(a, b, c)$	Example of a Galois $\mathbb{Q}$-Belyi map $\mathbb{P}^1 \to \mathbb{P}^1$
$(2, 2, c)$	D_c	$\frac{(\mathsf{s}^c+\mathsf{t}^c)^2}{4(\mathsf{st})^c}$
$(2, 3, 3)$	A_4	$\frac{(\mathsf{s}^2-2\mathsf{st}-2\mathsf{t}^2)^2(\mathsf{s}^4+2\mathsf{s}^3\mathsf{t}+6\mathsf{s}^2\mathsf{t}^2-4\mathsf{st}^3+4\mathsf{t}^4)^2}{2^6\mathsf{t}^3(\mathsf{s}-\mathsf{t})^3(\mathsf{s}^2+\mathsf{st}+\mathsf{t}^2)^3}$
$(2, 3, 4)$	S_4	$\frac{-(4\mathsf{st})^2(\mathsf{s}^2-3\mathsf{t}^2)^2(\mathsf{s}^4+6\mathsf{s}^2\mathsf{t}^2+81\mathsf{t}^4)^2(3\mathsf{s}^4+2\mathsf{s}^2\mathsf{t}^2+3\mathsf{t}^4)^2}{(s^2+3\mathsf{t}^2)^4(s^4-18\mathsf{s}^2\mathsf{t}^2+9\mathsf{t}^4)^4}$
$(2, 3, 5)$	A_5	$\frac{-(3^4\mathsf{s}^{10}+2^8\mathsf{t}^{10})^2(3^8\mathsf{s}^{20}-2^7 3^{10}\mathsf{s}^{15}\mathsf{t}^5-2^{18}3^{10}\mathsf{s}^{10}\mathsf{t}^{10}+2^{12}3^{10}\mathsf{s}^5\mathsf{t}^{15}+2^{16}\mathsf{t}^{20})^2}{(12\mathsf{st})^5(81\mathsf{s}^{10}-1584\mathsf{s}^5\mathsf{t}^5-256\mathsf{t}^{10})^5}$

3.1.3 The Belyi stack

In this section, we summarize a few geometric and arithmetic properties of the Belyi stack $\mathbb{P}^1(a,b,c)$. This is the relative stacky curve corresponding to Darmon's M-curve $(\mathbb{P}^1; 0, a; 1, b; \infty, c)$ in [12].

Situation 3.1.3.a. Here:

- We use $\mathbf{e} := (e_0, e_1, e_\infty) = (a,b,c) \in \mathbb{Z}^3$ be a triple of positive integers.
- $\mathbb{P}^1 = \operatorname{Proj} \mathbb{Z}[\mathsf{s},\mathsf{t}]$.
- Let $D_0 = V(\mathsf{s}), D_1 = V(\mathsf{s}-\mathsf{t}), D_\infty = V(\mathsf{t}) \in \operatorname{Div}(\mathbb{P}^1_{\mathbb{Z}})$.

Definition 3.1.3.b (Belyi stack)**.** We define the Belyi stack $\mathbb{P}^1(a,b,c)$ as the iterated root stack of $\mathbb{P}^1_{\mathbb{Z}}$ at the divisor $D := a \cdot D_0 + b \cdot D_1 + c \cdot D_\infty$. In the notation of Section 2.3, we have

$$\mathbb{P}^1(a,b,c) := \left(\sqrt[a]{\mathbb{P}^1; D_0}\right) \times_{\mathbb{P}^1} \left(\sqrt[b]{\mathbb{P}^1; D_1}\right) \times_{\mathbb{P}^1} \left(\sqrt[c]{\mathbb{P}^1; D_\infty}\right).$$

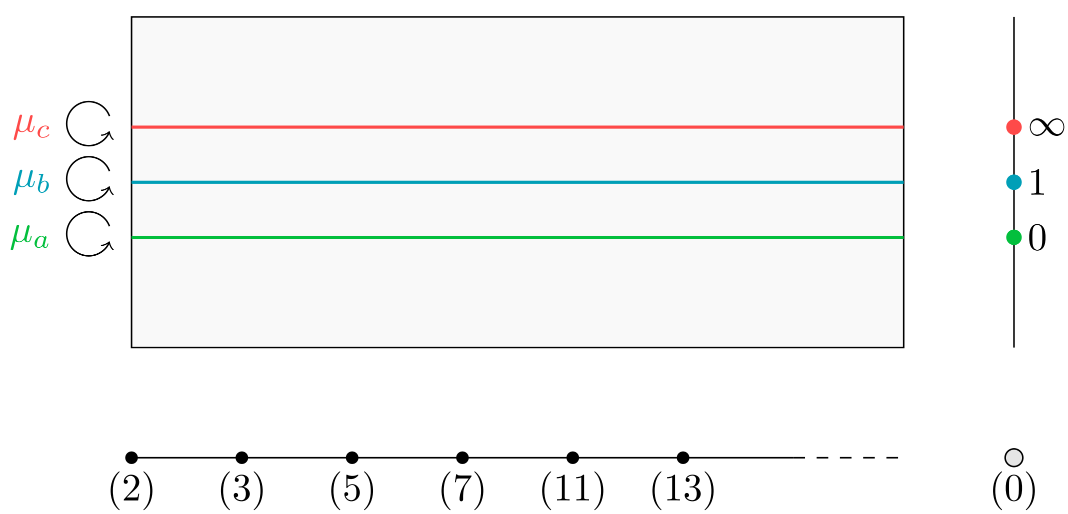


Figure 3.1: The Belyi stack of signature (a,b,c).

We start by summarizing some straightforward geometric properties of the Belyi stack.

Lemma 3.1.3.c. *Suppose we are in Situation 3.1.3.a. Then*

(i) The Belyi stack $\mathbb{P}^1(a,b,c)$ is a relative stacky curve over $\mathbb{Z}$ with coarse space $\mathbb{P}^1$, in the sense of [38, Definition 11.2.1]. The coarse space morphism $\pi\colon \mathbb{P}^1(a,b,c) \to \mathbb{P}^1$ is an isomorphism over the open set $U = \mathbb{P}^1 - D_0 \cup D_1 \cup D_\infty$.

(ii) Let $R = \mathbb{Z}[1/abc]$. Then the base change $\mathbb{P}^1(a,b,c)_R$ is tame.

(iii) For every closed point s in $\operatorname{Spec} R$, the fiber $\mathbb{P}^1(a,b,c)_s$ is a stacky curve over the residue field $\mathbf{k}(s)$, in the sense of [38, Definition 5.2.1]. Moreover, the Euler characteristic of $\mathbb{P}^1(a,b,c)_s$ is

$$\chi(\mathbb{P}^1(a,b,c)_s) = \tfrac{1}{a} + \tfrac{1}{b} + \tfrac{1}{c} - 1. \tag{3.3}$$

We define this common value to be the Euler characteristic of $\mathbb{P}^1(a,b,c)$.

Proof. (i) These follow by standard properties of root stacks [25, Theorem 10.3.10]. See also Section 2.3. (ii) For every point $s\colon \operatorname{Spec} K \to R$, the characteristic of K does not divide abc. Since $\mathbb{P}^1(a,b,c)_s$ is the iterated root stack of $\mathbb{P}^1_K$ at the divisor $a\cdot 0 + b\cdot 1 + c\cdot\infty \in \operatorname{Div}(\mathbb{P}^1_K)$, it is tame. (iii) For every point $s\colon \operatorname{Spec} K \to R$, let $\mathcal{X} = \mathbb{P}^1(a,b,c)_s$ be the corresponding stacky curve over K. From [38, Proposition 5.5.6] and the discussion thereafter, we know that

$$g(\mathcal{X}) = g(\mathbb{P}^1_K) + \frac{1}{2}\left(1 - \frac{1}{G_0} + 1 - \frac{1}{G_1} + 1 - \frac{1}{G_\infty}\right) = \tfrac{1}{2}\left(3 - \tfrac{1}{a} - \tfrac{1}{b} - \tfrac{1}{c}\right),$$

and thus

$$\chi(\mathcal{X}) = 2 - 2g(\mathcal{X}) = \tfrac{1}{a} + \tfrac{1}{b} + \tfrac{1}{c} - 1.$$

□

We now turn to the arithmetic of the Belyi stack. We want to understand the set of $\mathbb{Z}$-points on $\mathbb{P}^1(a,b,c)$. We have already done most of the work in Proposition 2.3.3.d. Recall the definition of the intersection ideal of two points from Definition 2.3.3.b.

Lemma 3.1.3.d (R-points on the Belyi stack)**.** *Let R be a principal ideal domain with fraction field k. Let $\mathbb{P}^1(a,b,c)$ be the base extension of the Belyi stack to R. The set $\mathbb{P}^1(a,b,c)\langle R\rangle$ is in bijection with the subset of $Q = (s:t) \in \mathbb{P}^1(R) = \mathbb{P}^1(k)$ such that $Q \in \{D_0, D_1, D_\infty\}$, or:*

- *$I(0,Q) = \langle s\rangle$ is a a^{th} power.*
- *$I(1,Q) = \langle s-t\rangle$ is a b^{th} power.*
- *$I(\infty,Q) = \langle t\rangle$ is a c^{th} power.*

Proof. From the definition of fiber product of groupoids (see [25, Section 3.4.9]), it follows that the set $\mathbb{P}^1(a,b,c)\langle R\rangle$ is the fiber product set

$$\left(\sqrt[a]{\mathbb{P}^1;0}\right)\langle R\rangle \times_{\mathbb{P}^1(R)} \left(\sqrt[b]{\mathbb{P}^1;1}\right)\langle R\rangle \times_{\mathbb{P}^1(R)} \left(\sqrt[c]{\mathbb{P}^1;\infty}\right)\langle R\rangle,$$

so the result follows from the description of the R-points of the n^{th} root stack of the projective line at a given point P. See the proof of Proposition 2.3.3.d for the details. □

The fundamental group of the Belyi orbifold $\mathbb{P}^1(a,b,c)(\mathbb{C})$ is a familiar one: the triangle group $\bar{\triangle}(a,b,c)$, as defined in Section 3.1.1. Indeed, the fundamental group of the thrice-punctured Riemann sphere $\mathbb{CP}^1 - \{0,1,\infty\}$ is the free group on three generators; these generators are represented by loops $\gamma_0, \gamma_1, \gamma_\infty$ going around the punctures. Introducing the stackyness imposes the relations

$$\gamma_0^a = \gamma_1^b = \gamma_\infty^c = \gamma_0\gamma_1\gamma_\infty = 1$$

on the generators.

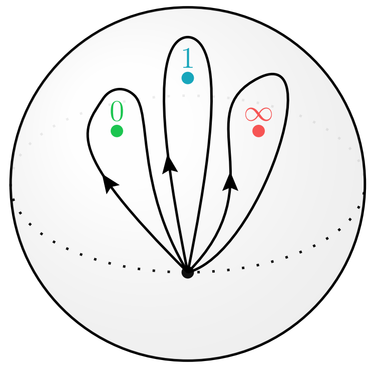


Figure 3.2: Generators of the fundamental group of the orbifold $\mathbb{P}^1(a,b,c)(\mathbb{C})$.

More generally, the fundamental groups of any orbifold curve can be calculated via van Kampen's theorem [4, Proposition 5.6]. It would be desirable to translate these results to their algebraic analogs. For our applications, it will be enough to confirm the existence of Galois étale covers $Z \to \mathbb{P}^1(a,b,c)$ realizing the Belyi stack as the quotient of a curve by a finite group.

The definition of the Belyi stack implies the following.

Lemma 3.1.3.e. *Let $\phi\colon Z_K \to \mathbb{P}^1_K$ be a geometrically Galois K-Belyi map of signature (a,b,c). Then, there exists an étale $\mathrm{Aut}(\phi)$-torsor $\psi\colon Z_K \to \mathbb{P}^1(a,b,c)_K$ such that Diagram (3.4) commutes.*

$$\begin{array}{ccc} Z_K & \overset{\psi}{\underset{\text{étale } \mathrm{Aut}(\phi)\text{-torsor}}{\dashrightarrow}} & \\ \text{geometrically Galois Belyi } \Big\downarrow \phi & & \mathbb{P}^1(a,b,c)_K \\ & \swarrow_{\text{coarse}} & \\ \mathbb{P}^1_K\,. & & \end{array} \tag{3.4}$$

3.2 The Fermat stack

Situation 3.2.0.a. Here:

- k is a number field, with ring of integers $\mathcal{O}_k$.
- $\mathbf{c} := (A, B, C) \in \mathbb{Z}^3$ is a triple of coefficients, satisfying $A \cdot B \cdot C \neq 0$.
- $\mathbf{e} := (a, b, c) \in \mathbb{Z}^3$ is a triple of strictly positive exponents, called a signature.
- Let $m := \gcd(bc, ac, bc)$ and $d := \gcd(a, b, c)$. We define the weight vector associated to the signature $\mathbf{e}$ to be

$$\mathbf{w} := (w_0, w_1, w_\infty) = (bc/m, ac/m, ab/m). \tag{3.5}$$

- $F\colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0$ is the generalized Fermat equation with coefficients $\mathbf{c}$ and signature $\mathbf{e}$.
- $\mathcal{S}$ denotes the set of rational primes p such that $p \mid a \cdot b \cdot c$ or $p \mid A \cdot B \cdot C$.

To every generalized Fermat equation F we associate a graded ring $\mathcal{R} = \mathcal{R}_F$, a punctured cone $\mathcal{U} = \mathcal{U}_F$, and a group scheme $\mathbb{G}_{\mathrm{m}}(\mathbf{w})$ equipped with a natural action on $\mathcal{U}$. In this section we study the scheme quotient $\mathcal{U}/\mathbb{G}_{\mathrm{m}}(\mathbf{w})$ and the stack quotient $[\mathcal{U}/\mathbb{G}_{\mathrm{m}}(\mathbf{w})]$. The advantage of this quotient is that it embeds in the weighted projective stack $\mathcal{P}(\mathbf{w})$. One can take the quotient of $\mathcal{U}$ by a bigger group H. We do this in Section 3.3.

3.2.1 The graded ring

Definition 3.2.1.a (Graded ring associated to a GFE)**.** The graded ring associated to F is

$$\mathcal{R} := \mathbb{Z}[\mathsf{x}, \mathsf{y}, \mathsf{z}]/\langle F \rangle,$$

where x has degree w_0, y has degree w_1 and z has degree w_∞. The irrelevant ideal of $\mathcal{R}$ is denoted by $\mathcal{R}_+ := \bigoplus_{n>0} \mathcal{R}_n$.

Definition 3.2.1.b (Punctured cone associated to a GFE)**.** The punctured cone associated to F is

$$\mathcal{U} := \operatorname{Spec}\mathcal{R} - V(\mathcal{R}_+),$$

where $V(I)$ denotes the closed subset associated to the ideal $I \subset \mathcal{R}$.

The graded structure of $\mathcal{R}$ induces an action of the multiplicative group $\mathbb{G}_{\mathrm{m}} := \operatorname{Spec}\mathbb{Z}_k[u, u^{-1}]$ on the scheme $\mathcal{U}$. On points, this action is given by

$$(x, y, z) \cdot \lambda = (\lambda^{w_0} x, \lambda^{w_0} y, \lambda^{w_\infty} z). \tag{3.6}$$

Definition 3.2.1.c. Let $\mathbb{G}_{\mathrm{m}}(\mathbf{w})$ be the group scheme over $\operatorname{Spec}\mathbb{Z}$ given by the image of the homomorphism $\mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^3 : \lambda \mapsto (\lambda^{w_0}, \lambda^{w_0}, \lambda^{w_\infty})$.

Remark 3.2.1.d. Note that our choice of $\mathbf{w}$ ensures that $\mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}(\mathbf{w})$ is injective. Indeed, $\ker(\mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}(\mathbf{w}))$ equals $\mu_{\gcd(w_0, w_1, w_\infty)}$, and $\gcd(w_0, w_1, w_\infty) = 1$ by construction.

Taking the scheme quotient of the punctured cone $\mathcal{U}$ by the group $\mathbb{G}_{\mathrm{m}}(\mathbf{w})$ we obtain the scheme $\mathsf{C} := \operatorname{Proj}\mathcal{R}$. We show that $\mathsf{C} \subset \mathbb{P}^2_{\mathbb{Z}}$ is isomorphic to the relative curve given by the equation $A\mathsf{x}^d + B\mathsf{y}^d + C\mathsf{z}^d = 0$.

Lemma 3.2.1.e. *We have* $\operatorname{Proj}\mathcal{R} \cong \operatorname{Proj}\mathbb{Z}[X, Y, Z]/\langle AX^d + BY^d + CZ^d\rangle$, *where* $d = \gcd(a, b, c)$ *and* $\deg X = \deg Y = \deg Z = 1$.

Proof. By [17, Proposition 2.4.7], we have that $\operatorname{Proj}\mathcal{R} \cong \operatorname{Proj}\mathcal{R}^{(n)}$ for every $n > 0$. Choose $n := l/d$ where $l = \operatorname{lcm}(a, b, c)$ and $d = \gcd(a, b, c)$. Consider the elements $X := \mathsf{x}^{a/d}, Y := \mathsf{y}^{b/d}$, and $Z := \mathsf{z}^{c/d}$. Observe that $X, Y, Z \in \mathcal{R}_1^{(n)} = \mathcal{R}_n$ and $F = AX^d + BY^d + CZ^c$. From Bézout's identity, it follows that in fact $\mathcal{R}^{(n)} = \mathbb{Z}[X, Y, Z]/\langle AX^d + BY^d + CZ^d\rangle$, and this concludes the proof. ☐

3.2.2 The stacky proj

The Proj functor forgets important data from the graded ring. Taking the stack quotient of $\mathcal{U}$ by $\mathbb{G}_{\mathrm{m}}(\mathbf{w})$ instead of the scheme quotient we are able to retain this information. Recall the stacky proj construction [25, Example 10.2.8].

Definition 3.2.2.a (Fermat stack associated to a GFE)**.** The Fermat associated to F is

$$\mathcal{C} := \mathbf{Proj}\,\mathcal{R} := [\mathcal{U}/\mathbb{G}_{\mathrm{m}}(\mathbf{w})].$$

$\mathcal{C}$ is a closed substack of the weighted projective stack $\mathcal{P}(\mathbf{w}) := [(\mathbb{A}^3 - \mathbf{0})/\mathbb{G}_{\mathrm{m}}(\mathbf{w})]$.

Lemma 3.2.2.b. *Let $\mathcal{C}$ be the Fermat stack associated to a generalized Fermat equation F. Then,*

(i) $\mathcal{C}$ is cyclotomic stack over $\mathbb{Z}$, in the sense of [1, Definition 2.3.1].

(ii) The projective scheme $\mathsf{C} := \operatorname{Proj} \mathbb{Z}[X,Y,Z]/\langle AX^d + BX^d + CZ^d\rangle$ is the coarse moduli space of $\mathcal{C}$.

(iii) Let $\mathcal{S}$ be the finite set of bad primes defined in Situation 3.2.0.a and let R be the ring of $\mathcal{S}$-integers $\mathbb{Z}_{\mathcal{S}}$. Then $\mathcal{C}_R$ is a tame stacky curve over R in the sense of [38, Definition 11.2.1].

(iv) The coarse map $\pi\colon \mathcal{C}_R \to \mathsf{C}_R$ restricts to an isomorphism above the open set $U = \mathsf{C}_R - Q_0 \cup Q_1 \cup Q_\infty$, where $Q_0 = V(X), Q_1 = V(Y)$, and $Q_\infty = V(Z)$. Consequently, $\mathcal{C}_R$ is isomorphic to the iterated root stack of C at the divisor

$$m_0 \cdot Q_0 + m_1 \cdot Q_1 + m_\infty \cdot Q_\infty, \tag{3.7}$$

where the multiplicities m_0, m_1, and m_∞ are given by Equation (3.8). In particular, $\mathcal{C}_R$ is a relative stacky curve over $\operatorname{Spec} R$ in the sense of [38, Definition

11.2.1].

Proof. (i) Indeed, $\mathbb{G}_{\mathrm{m}}$ acts properly on $\mathcal{U}$ via $\mathbb{G}_{\mathrm{m}}(\mathbf{w})$ with finite stabilizers (namely μ_m stabilizers). So, $\mathcal{C}$ is cyclotomic by [1, Example 2.3.2]. (ii) The coarse space of a quotient stack coincides with the coarse quotient. The result follows from Lemma 3.2.1.e. (iii) We need to verify that for every point $s\colon \operatorname{Spec} K \to R$, the base change $\mathcal{C}_s$ is a stacky curve over K. The Deligne–Mumford statement follows from [25, Corllary 8.4.2]. The smoothness follows from [35, Tag 0DLS]. The dimension statement follows from [35, Tag 0AFR]. The properness statement follows from the properness of the coarse map, the properness of $\mathsf{C}_K \to \operatorname{Spec} K$, and [25, Proposition 10.16.1]. Likewise, the geometric irreducibility statement follows from the geometric irreducibility of C_K, and the fact that the coarse map is a universal homeomorphism [10, Theorem 3.1].

(iv) This follows from (iii) and the fact that every tame relative stacky curve is an iterated root stack over the ramification divisor of its coarse map [31, Lemma 2.1]. To verify that these are the correct stabilizers, we may work over a geometric point $s\colon \operatorname{Spec} \bar{k} \to \operatorname{Spec} R$. Let $P = (x, y, z) \in \mathcal{U}(\bar{k})$. Suppose that $g = (\lambda^{w_0}, \lambda^{w_1}, \lambda^{w_\infty}) \in \mathbb{G}_{\mathrm{m}}(\mathbf{w})(\bar{k})$ stabilizes P. If $xyz \neq 0$, it follows that $g = (1, 1, 1)$. If $xyz = 0$, then only one coordinate can be zero. Suppose that $x = 0$. Then, we have that $\lambda^{w_1} = \lambda^{w_\infty} = 1$, which implies that $\lambda \in \mu_{w_1}(\bar{k}) \cap \mu_{w_\infty}(\bar{k}) = \mu_{\gcd(w_1,w_\infty)}(\bar{k})$. Let $w_0' \in \{0, \ldots, \gcd(w_1, w_\infty) - 1\}$ be the residue class of w_0 modulo $\gcd(w_1, w_\infty)$. Since $g = (\lambda^{w_0}, 1, 1)$, we conclude that $\operatorname{Stab}_{\mathbb{G}_{\mathrm{m}}(\mathbf{w})}(Q_0)$ has order

$$\begin{cases} \gcd(w_1, w_\infty)/w_0', & \text{if } w_0' \mid \gcd(w_1, w_\infty) \\ \gcd(w_1, w_\infty). & \text{otherwise.} \end{cases} \tag{3.8}$$

We obtain m_1 and m_∞ by analogous formulas. □

3.3 The group scheme H

For this section we will need some basic notions from the theory of diagonalizable group schemes of multiplicative type. See the notes of Oésterle [24] and Conrad [11, Appendix B].

Given a base scheme S, and a finitely generated $\mathbb{Z}$-module M, we define $\mathbf{D}_S(M)$ to be the S-group scheme $\operatorname{Spec} \mathcal{O}_S[M]$ representing the functor $\underline{\operatorname{Hom}}_{S-\mathtt{GrpSch}}(M_S, \mathbb{G}_{\mathrm{m}})$ of characters of the constant S-group scheme M_S. An S-group scheme is called diagonalizable if it is isomorphic to $\mathbf{D}_S(M)$ for some finitely generated $\mathbb{Z}$-module M. Moreover, $\mathbf{D}_S$ gives a contravariant functor between finitely generated $\mathbb{Z}$-modules and the category of diagonalizable S-group schemes satisfying certain exactness properties that are summarized in [24, 5.3].

Situation 3.3.0.a. Let

- $\mathbf{D}$ denote the functor described above, over the base scheme $S = \operatorname{Spec} \mathbb{Z}$.
- (a, b, c) be a triple of positive integers.
- $m := \gcd(bc, ac, ab)$, and define the weight vector of (a, b, c) by $\mathbf{w} = (w_0, w_1, w_\infty)$, where $w_0 = bc/m$, $w_1 = ac/m$ and $w_\infty = ab/m$.
- $\mathbb{G}_{\mathrm{m}}(\mathbf{w})$ be the image of the (injective) homomorphism $\mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^3$ given by $\lambda \mapsto (\lambda^{w_0}, \lambda^{w_1}, \lambda^{w_\infty})$.
- $\bar{\triangle}(a, b, c)$ denote the triangle group

$$\bar{\triangle}(a, b, c) = \langle \gamma_0, \gamma_1, \gamma_\infty : \gamma_0^a = \gamma_1^b = \gamma_\infty^c = \gamma_0\gamma_1\gamma_\infty = 1 \rangle.$$

Definition 3.3.0.b. Consider the finitely generated $\mathbb{Z}$-module

$$M := \langle (a, -b, 0), (0, b, -c), (-a, 0, c) \rangle \subset \mathbb{Z}^3. \tag{3.9}$$

Define H to be the subgroup $\mathbf{D}(\mathbb{Z}^3/M)$ of $\mathbb{G}_{\mathrm{m}}^3 = \mathbf{D}(\mathbb{Z}^3)$.

The diagonalizable group H admits a maximal torus corresponding to the $\mathbb{Z}$-free part of $\mathbb{Z}^3/M$. Moreover, we have the following characterization. An important formula to keep in mind is

$$\operatorname{lcm}(a, b, c) = \frac{abc}{\gcd(bc, ac, ab)}. \tag{3.10}$$

Lemma 3.3.0.c (The structure of H)**.** *Let* $\mathsf{K} = \mathbf{D}(\bar{\triangle}(a, b, c)^{\mathsf{ab}})$*, and recall that* $m = \gcd(bc, ac, ab)$*.*

1. The $\mathbb{Z}$*-module* $\mathbb{Z}^3/M$ *is isomorphic to* $\mathbb{Z} \oplus \bar{\triangle}(a, b, c)^{\mathsf{ab}}$*.*

2. Let K *be the kernel of the map*

$$\mu_a \times \mu_b \times \mu_c \to \mu_{\operatorname{lcm}(a,b,c)}, \quad (\xi_0, \xi_1, \xi_\infty) \mapsto \xi_0 \cdot \xi_1 \cdot \xi_\infty.$$

Then $\mathsf{K} \cong \mathbf{D}(\bar{\triangle}(a, b, c)^{\mathsf{ab}})$*.*

3. The group scheme H *is equal to* $\mathbb{G}_m(\mathbf{w}) \cdot \mathsf{K}$ *and isomorphic to* $\mathbb{G}_m \times \mathsf{K}$*.*

4. In particular, when $m = 1$*,* $\mathsf{H} = \mathbb{G}_m(\mathbf{w}) \cong \mathbb{G}_m$*.*

Proof. (1) We calculate the invariant factor decomposition of $\mathbb{Z}^3/M$ from the Smith normal form of the matrix having the generators of M as its rows [36, Theorem 2.3]. Let

$$\mathsf{m} = \begin{bmatrix} a & -b & 0 \\ 0 & b & -c \\ -a & 0 & c \end{bmatrix}.$$

From Stanley's formula [36, Theorem 2.4], we see that

$$\mathrm{SNF}(\mathsf{m}) = \begin{bmatrix} d & 0 & 0 \\ 0 & m/d & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

where $d = \gcd(a, b, c)$ is the greatest common divisor of the 1×1 minors, and $m = \gcd(bc, ac, ab)$ is the greatest common divisor of the 2×2 minors. It follows that $\mathbb{Z}^3/M \cong \mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/(m/d)\mathbb{Z}$.

It remains to show that $\mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/(m/d)\mathbb{Z}$ is isomorphic to $\bar{\triangle}(a, b, c)^{\mathsf{ab}}$. To this end, note that the group $\bar{\triangle}(a, b, c)^{\mathsf{ab}}$ is isomorphic to the quotient of $\mathbb{Z}^3$ by the subgroup

$$J = \langle (a, 0, 0), (0, b, 0), (0, 0, c), (1, 1, 1) \rangle.$$

As before, we calculate the invariant factor decomposition of $\mathbb{Z}^3/J$ via a Smith normal form computation.

$$\mathrm{SNF} \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & m/d \\ 0 & 0 & 0 \end{bmatrix}.$$

We conclude that $\bar{\triangle}(a, b, c)^{\mathsf{ab}} \cong \mathbb{Z}^3/J \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/(m/d)\mathbb{Z}$.

(2) From the presentation given in Situation 3.3.0.a, we see that $\bar{\triangle}(a, b, c)^{\mathsf{ab}}$ is the cokernel of the map $\mathbb{Z}/l\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z} \oplus \mathbb{Z}/c\mathbb{Z}$ taking $1 \bmod l \mapsto (1 \bmod a, 1 \bmod b, 1 \bmod c)$, where $l = \mathrm{lcm}(a, b, c)$. The result follows by applying the functor $\mathbf{D}$.

(3) The computation above shows that $\mathbb{Z}^3/M$ has $\mathbb{Z}$-rank one. The free part of $\mathbb{Z}^3/M$ corresponds to the (dual of the) kernel of the matrix m. That is, we want a

generator for the subgroup of $\mathbf{v} \in \mathbb{Z}^3$ such that

$$\begin{bmatrix} a & -b & 0 \\ 0 & b & -c \\ -a & 0 & c \end{bmatrix} \mathbf{v} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

In other words, we are looking for minimal $v_1, v_2, v_3 \in \mathbb{Z}$ satisfying $av_1 = bv_2 = cv_3$. But this is precisely the property defining the weight vector $\mathbf{w}$ (see Situation 3.3.0.a). The equality $\mathsf{H} = \mathbb{G}_{\mathrm{m}}(\mathbf{w}) \cdot \mathsf{K}$ follows from the exact sequence $0 \to \mathbb{Z}^3/\langle \mathbf{w} \rangle \to \mathbb{Z}^3/M \to \mathbb{Z}^3/J \to 0$ and the exactness of the functor $\mathbf{D}$.

The statement that $\mathsf{H} \cong \mathbb{G}_{\mathrm{m}} \times \mathsf{K}$ follows from the fact that $\mathbb{Z}^3/\langle \mathbf{w} \rangle$ has $\mathbb{Z}$-rank one and the general fact that $\mathbf{D}(M_1 \oplus M_2) \cong \mathbf{D}(M_1) \times \mathbf{D}(M_2)$ for arbitrary finitely generated $\mathbb{Z}$-modules M_1, M_2. □

Lemma 3.3.0.d. *Let $\mathcal{S}$ be a finite set of rational primes, and let $R = \mathbb{Z}[\mathcal{S}^{-1}]$. Then $\mathrm{H}^1(R, \mathsf{H}_R)$ is finite. Moreover, $\mathrm{H}^1(\mathbb{Z}, \mathsf{H})$ is trivial.*

Proof. From $\mathsf{H} \cong \mathbb{G}_{\mathrm{m}} \times \mathsf{K}$, we obtain the exact sequence $\mathrm{H}^1(R, \mathbb{G}_{\mathrm{m}}) \to \mathrm{H}^1(R, \mathsf{H}) \to \mathrm{H}^1(R, \mathsf{K}) \to \mathrm{H}^2(R, \mathbb{G}_{\mathrm{m}})$. Since both $\mathrm{H}^1(R, \mathbb{G}_{\mathrm{m}}) = \operatorname{Pic} \mathbb{Z}$ is trivial, we have that $\mathrm{H}^1(R, \mathsf{H})$ injects into the finite group $\mathrm{H}^1(R, \mathsf{K})$. In the special case of $R = \mathbb{Z}$, $\mathrm{H}^2(\mathbb{Z}, \mathbb{G}_{\mathrm{m}}) = \operatorname{Br} \mathbb{Z}$ is also trivial, and we obtain that $\mathrm{H}^1(\mathbb{Z}, \mathsf{H}) \cong \mathrm{H}^1(\mathbb{Z}, \mathsf{K})$. But Minkowski's theorem implies that $\mathrm{H}^1(\mathbb{Z}, \mathsf{K})$ is trivial. □

3.4 The Belyi stack as a quotient

Situation 3.4.0.a. We place ourselves in the following situation for the remainder of this section.

- Let $F := \operatorname{Spec} \mathbb{Z}[\mathsf{x}, \mathsf{y}, \mathsf{z}]/\langle A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c \rangle \subset \mathbb{A}^3$.
- Let $\mathcal{T}$ be set of primes dividing the integer $a \cdot b \cdot c \cdot A \cdot B \cdot C$.

- Let $R = \mathbb{Z}[\mathcal{T}^{-1}]$ be the ring of $\mathcal{T}$-integers.
- Let H be the affine group scheme introduced in Definition 3.3.0.b.
- Let $\mathcal{U}$ be the punctured cone associated to F, defined over R.
- Let $s\colon \operatorname{Spec} k \to \operatorname{Spec} R$ denote a geometric point.
- For a geometric object $\mathcal{X}$ defined over R, we let $\mathcal{X}_s := \mathcal{X} \times_s \operatorname{Spec} k$ denote the geometric fiber above s.

In the author's view, the following theorem is the central result in the theory of generalized Fermat equations. It serves as the starting point for a substantial portion of the main results in the field.

Theorem 3.4.0.b. *The map*

$$j\colon \mathcal{U} \to \mathbb{P}^1_R, \quad (x, y, z) \mapsto (-Ax^a : Cz^c) \tag{3.11}$$

induces an isomorphism $\mathbf{j}\colon [\mathcal{U}/\mathsf{H}_R] \cong \mathbb{P}^1(a,b,c)_R$.

The reason we are interested in the group scheme H is that it arises as the stabilizer in $\mathbb{G}_{\mathrm{m}}^3$ of the punctured cone $\mathcal{U}$ associated to a generalized Fermat equation.

Lemma 3.4.0.c. *Let* S *be the stabilizer subgroup of* $\mathcal{U}$ *under the action of* $\mathbb{G}_m^3$ *on* $\mathbb{A}^3_{\mathbb{Z}}$. *Then,* $\mathsf{H} \subset \mathsf{S}$ *and* $\mathsf{H}_R = \mathsf{S}_R$.

Proof. By definition, $\mathsf{S} := \operatorname{Stab}_{\mathbb{G}_{\mathrm{m}}^3}(\mathcal{U})$ is the group scheme that takes any $\mathbb{Z}$-algebra B to the group

$$\mathsf{S}(B) = \left\{(\lambda_0, \lambda_1, \lambda_\infty) \in (B^\times)^3 : F(\lambda_0\mathsf{x}, \lambda_1\mathsf{y}, \lambda_\infty\mathsf{z})/F(\mathsf{x},\mathsf{y},\mathsf{z}) \in B^\times\right\},$$

and this group visibly contains

$$\mathsf{H}(B) = \left\{(\lambda_0, \lambda_1, \lambda_\infty) \in (B^\times)^3 : \lambda_0^a = \lambda_1^b = \lambda_\infty^c\right\}.$$

So we have an inclusion $\mathsf{H} \hookrightarrow \mathsf{S}$. For every geometric point $s\colon \operatorname{Spec} k \to \operatorname{Spec} R$, this inclusion pulls back to an equality $\mathsf{S}_s = \mathsf{H}_s$, so we conclude that $\mathsf{S}_R = \mathsf{H}_R$ by fpqc descent [35, Tag 02L4] and spreading out. □

We start by considering the situation on the geometric fibers.

Lemma 3.4.0.d. *For every geometric point $s\colon \operatorname{Spec} k \to \operatorname{Spec} R$, the map*

$$j\colon \mathcal{U}_s \to \mathbb{P}^1_s, \quad (x, y, z) \mapsto (-Ax^a : Cz^c) \tag{3.12}$$

induces an isomorphism $\mathbf{j}_s\colon [\mathcal{U}_s/\mathsf{H}_s] \cong \mathbb{P}^1(a, b, c)_s$.

Proof. We omit the subscript "s" and work over k throughout. We start by showing that j induces a coarse map $j\colon [\mathcal{U}/\mathsf{H}] \to \mathbb{P}^1$. Recall that $\mathcal{R} = k[\mathsf{x}, \mathsf{y}, \mathsf{z}]/\langle A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c\rangle$ is the coordinate ring of F. Consider the affine open $D(\mathsf{z}) \subset F$, with corresponding coordinate ring $\mathcal{R}[1/\mathsf{z}]$. Note that $\mathcal{U} \cap D(\mathsf{z}) = D(\mathsf{z})$. Since $D(\mathsf{z}) = \operatorname{Spec} \mathcal{R}[1/\mathsf{z}]$ is affine, H is linearly reductive, and $[D(\mathsf{z})/\mathsf{H}]$ is tame, the natural map $[\operatorname{Spec} \mathcal{R}[1/\mathsf{z}]/\mathsf{H}] \to \operatorname{Spec} \mathcal{R}[1/\mathsf{z}]^H$ is a good moduli space and thus a coarse moduli space (see [2, Theorem 13.2 and Remark 7.3]). Now, we calculate that $\mathcal{R}[1/\mathsf{z}]^H = k\left[\frac{-A\mathsf{x}^a}{C\mathsf{z}^c}\right]$. Applying the same argument to $D(\mathsf{x})$, the result follows by glueing the maps

$$[\mathcal{U} \cap D(\mathsf{x})/\mathsf{H}] \to \operatorname{Spec} k\left[\tfrac{-C\mathsf{z}^c}{A\mathsf{x}^a}\right], \quad [\mathcal{U} \cap D(\mathsf{z})/\mathsf{H}] \to \operatorname{Spec} k\left[\tfrac{-A\mathsf{x}^a}{C\mathsf{z}^c}\right]$$

to obtain the coarse map $j\colon [\mathcal{U}/\mathsf{H}] \to \mathbb{P}^1$.

We proceed to show that $[\mathcal{U}/\mathsf{H}] \cong \mathbb{P}^1(a, b, c)$. By definition of $\mathbb{P}^1(a, b, c)$ as an iterated root stack, the map $j\colon \mathcal{U} \to \mathbb{P}^1$ induces a map $\mathbf{j}\colon [\mathcal{U}/\mathsf{H}] \to \mathbb{P}^1(a, b, c)$. Indeed, the map $j\colon \mathcal{U} \to \mathbb{P}^1$ satisfies

$$j^*\mathcal{O}_{\mathbb{P}^1}(-P_0) = \mathcal{L}_0^a, \quad j^*\mathcal{O}_{\mathbb{P}^1}(-P_1) = \mathcal{L}_1^b, j^*\mathcal{O}_{\mathbb{P}^1}(-P_\infty) = \mathcal{L}_\infty^c,$$

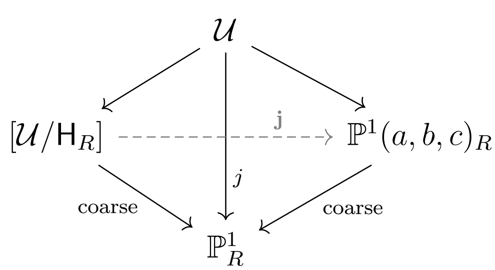
with $\mathcal{L}_0 = \mathsf{x}\cdot\mathcal{O}_{\mathcal{U}}, \mathcal{L}_1 = \mathsf{y}\cdot\mathcal{O}_{\mathcal{U}}$ and $\mathcal{L}_\infty = \mathsf{z}\cdot\mathcal{O}_{\mathcal{U}}$, and this gives rise an object in $\mathbb{P}^1(a,b,c)(\mathcal{U})$.

Since $[\mathcal{U}/\mathsf{H}]\langle k\rangle = \mathbb{P}^1(k) = \mathbb{P}^1(a,b,c)\langle k\rangle$, and the map $[\mathcal{U}/\mathsf{H}](k) \to \mathbb{P}^1(a,b,c)(k)$ induces isomorphisms between the stabilizer groups of the stacky points

$$\begin{aligned}\mathrm{Stab}_{\mathsf{H}}(V(\mathsf{x})) &\cong \mu_a(k),\\ \mathrm{Stab}_{\mathsf{H}}(V(\mathsf{y})) &\cong \mu_b(k),\\ \mathrm{Stab}_{\mathsf{H}}(V(\mathsf{z})) &\cong \mu_c(k).\end{aligned}$$

The result follows from [38, Lemma 5.3.10(a)]. □

Proof of Theorem 3.4.0.b. The R-morphism j is surjective (this can be checked on geometric fibers by fpqc descent [35, Tag 02KV] and spreading out) and H_R-invariant. From Lemma 2.2.4.c, this induces a morphism $[\mathcal{U}/\mathsf{H}_R] \to \mathbb{P}^1_R$, which factors through the coarse map $\mathbb{P}^1(a,b,c)_R \to \mathbb{P}^1_R$ by the definition of the Belyi stack. Both $\mathbb{P}^1(a,b,c)_R$ and $[\mathcal{U}/\mathsf{H}_R]$ are tame relative stacky curves. To calculate the coarse space of $\mathcal{U}/\mathsf{H}$ of $[\mathcal{U}/\mathsf{H}]$, we use the same argument as in the proof of Lemma 3.4.0.d.



In summary, we have a morphism $\mathbf{j}\colon [\mathcal{U}/\mathsf{H}]_R \to \mathbb{P}^1(a,b,c)_R$ with the property that on each geometric fiber, the induced map on the coarse spaces $(\mathcal{U}/\mathsf{H})_s \to \mathbb{P}^1_s$

is an isomorphism inducing a stabilizer-preserving bijection between $[\mathcal{U}/\mathsf{H}]\langle\bar{k}\rangle$ and $\mathbb{P}^1(a,b,c)\langle\bar{k}\rangle$. [38, Lemma 5.3.10 (a)] implies that $(\widetilde{j})_s$ is an isomorphism for every geometric point of $\operatorname{Spec} R$, and this implies that the same is true globally.

Alternatively, we can apply Santens' characterization of tame relative stacky curves [31, Lemma 2.1]. □

3.5 The method of descent on the Belyi stack

Situation 3.5.0.a. Here

- $\mathcal{S}$ is a finite set of places in a number field k, containing the archimedean places.
- $\mathcal{O}_{\mathcal{S}}$ is the ring of $\mathcal{S}$-integers of k.
- G is a finite fppf group scheme over $\operatorname{Spec} \mathcal{O}_{\mathcal{S}}$.
- We abbreviate $\mathrm{H}^1(\mathcal{O}_{\mathcal{S}}, G) = \check{\mathrm{H}}^1_{\mathtt{fppf}}(\mathcal{O}_{\mathcal{S}}, G)$, as in Section 2.2.1.

The finiteness results presented in this section rely crucially on the finiteness of the cohomology sets $\mathrm{H}^1(\mathcal{O}_{\mathcal{S}}, G)$. Let $\mathrm{H}^1_{\mathcal{S}}(k, G(\bar{k}))$ denote the subset of the Galois cohomology set $\mathrm{H}^1(k, G(\bar{k}))$ of cohomology classes unramified outside of $\mathcal{S}$, as in [28, Section 6.5.7]. See also [28, Exercises 8.4 and 8.5].

Theorem 3.5.0.b. *The following statements hold.*

1. *There is an isomorphism of pointed sets* $\mathrm{H}^1(\mathcal{O}_{\mathcal{S}}, G) \cong \mathrm{H}^1_{\mathcal{S}}(k, G(\bar{k}))$. *This isomorphism sends the class of a G-torsor $T \to \operatorname{Spec} R$ to the class of the G_k-torsor $T_k \to \operatorname{Spec} k$.*

2. *The set* $\mathrm{H}^1(\mathcal{O}_{\mathcal{S}}, G)$ *is finite.*

Working with $\mathrm{H}^1_{\mathcal{S}}(k, G(\bar{k}))$ instead of $\mathrm{H}^1(\mathcal{O}_{\mathcal{S}}, G)$ allows us to work over k. In practice, this is useful for computing the twists with Galois cohomology.

Theorem 3.5.0.c (Integral descent on the Belyi stack)**.** *Let* $\varphi\colon Z \to \mathbb{P}^1$ *be the* $\mathcal{O}_{\mathcal{S}}$ *integral model of a Galois Belyi map* $\varphi_k\colon Z_k \to \mathbb{P}^1_k$*, and let* $G := \mathrm{Aut}(\varphi)$ *be the automorphism group scheme. Denote by* $\phi\colon Z \to \mathbb{P}^1(a,b,c)$ *the corresponding étale cover. Then, the set of* $\mathcal{O}_{\mathcal{S}}$*-points on the Belyi stack* $\mathbb{P}^1(a,b,c)$ *is parametrized by the disjoint union of the images of the* $\mathcal{O}_{\mathcal{S}}$*-points of the twisted torsors* $\phi_\tau\colon : Z_\tau \to \mathbb{P}^1(a,b,c)$*. That is:*

$$\mathbb{P}^1(a,b,c)\langle \mathcal{O}_{\mathcal{S}}\rangle = \bigsqcup_{\tau \in \mathrm{H}^1(\mathcal{O}_{\mathcal{S}},G)} \phi_\tau(Z_\tau(\mathcal{O}_{\mathcal{S}})) = \bigsqcup_{\tau \in \mathrm{H}^1_{\mathcal{S}}(k,G(\bar{k}))} \varphi_\tau(Z_\tau(k)).$$

Proof. The first statement is a particular instance of Theorem 2.2.5.d. To verify the second equality in the displayed equation, recall that the valuative criterion of properness (see [28, Theorem 3.2.13]) implies that $Z(R) \cong Z(k)$ and $\mathbb{P}^1(R) \cong \mathbb{P}^1(k)$. Since $\mathbb{P}^1(a,b,c)\langle \mathcal{O}_{\mathcal{S}}\rangle \subset \mathbb{P}^1(\mathcal{O}_{\mathcal{S}})$, and the maps $\varphi_\tau\colon Z_\tau \to \mathbb{P}^1$ factors through ϕ_τ, we have that $\phi_\tau(Z(\mathcal{O}_{\mathcal{S}})) = \varphi_\tau(Z_\tau(k))$. □

3.5.1 The theorem of Darmon–Granville

In this section, we employ the method of descent on the Belyi stack $\mathbb{P}^1(a,b,c)$ to prove a celebrated theorem of Darmon and Granville [13, Theorem 2] in the setting of hyperbolic generalized Fermat equations. While this approach is essentially the same as the original proof, it has the advantage of being both more conceptual and more algorithmic.

Theorem 3.5.1.a (The Darmon–Granville theorem)**.** *Let*

$$F\colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0 \tag{3.13}$$

be a hyperbolic generalized Fermat equation with integer coefficients. Then, the set $\mathcal{U}(\mathbb{Z})$ *of primitive integer solutions to Equation* (3.13) *is finite.*

Proof. From Proposition 3.1.2.e, after replacing $\mathbb{Q}$ with a finite extension k, and choosing a large enough set of bad places $\mathcal{S}$, we can find an integral model of a geometrically Galois Belyi map $\varphi\colon Z \to \mathbb{P}^1$, with automorphism group scheme G, defined over the ring $\mathcal{O}_{\mathcal{S}}$. This map factors through the Belyi stack and induces an isomorphism $\mathbb{P}^1(a,b,c) \cong [Z/G]$ over $\operatorname{Spec} \mathcal{O}_{\mathcal{S}}$.

- First, $\mathrm{H}^1(\mathcal{O}_S, G)$ is finite (Theorem 3.5.0.b).

- Second, for each $\tau \in \mathrm{H}^1(\mathcal{O}_{\mathcal{S}}, G)$, the curves Z_k^τ are nice k-curves of genus $g > 1$. Indeed, the Hurwitz formula gives $\chi(Z) = \deg(\varphi)\chi(\mathbb{P}^1(a,b,c)) < 0$. In particular, the valuative criterion of properness ensures that $Z_\tau(\mathcal{O}_{\mathcal{S}}) = Z_\tau(k)$.

From the method of descent (Theorem 3.5.0.c), we have

$$\mathbb{P}^1(a,b,c)\langle \mathcal{O}_{\mathcal{S}} \rangle \cong \bigsqcup_{\tau \in \mathrm{H}^1_{\mathcal{S}}(k, G(\bar{k}))} \varphi_\tau(Z_\tau(k))$$

Faltings' theorem [16] implies that $Z_\tau(k)$ is finite for every τ, so $\mathbb{P}^1(a,b,c)\langle \mathcal{O}_{\mathcal{S}}\rangle$ is finite. But $\mathcal{U}(\mathbb{Z})/\mathsf{H}(\mathbb{Z})$ injects into $\mathbb{P}^1(a,b,c)\langle \mathcal{O}_{\mathcal{S}}\rangle$. Since $\mathsf{H}(\mathbb{Z})$ is finite, so is $\mathcal{U}(\mathbb{Z})$. □

3.5.2 The theorem of Beukers

In this section, we employ the method of descent to sketch a proof of a beautiful theorem of Beukers [7, Theorem 1.2]. Beukers proves a more general theorem (see [7, Theorem 1.5]) for Diophantine equations “arising from the invariant theory of finite matrix groups", of which the spherical generalized Fermat equations are a special case. It would be interesting to apply the method of descent (as in Theorem 2.2.5.d) to this setting as well.

Theorem 3.5.2.a (Beukers theorem)**.** *Let $F\colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0$ be a spherical generalized Fermat equation with integer coefficients. Then, the set $\mathcal{U}(\mathbb{Z})$ of primitive* *integer solutions is either infinite or empty. Furthermore, if a primitive integral solution exists, then there is a finite set of polynomials*

$$\{(\mathsf{x}_\tau(\mathsf{s},\mathsf{t}),\mathsf{y}_\tau(\mathsf{s},\mathsf{t}),\mathsf{z}_\tau(\mathsf{s},\mathsf{t}))\}_\tau \subset \mathbb{Z}[\mathsf{s},\mathsf{t}]^3$$

such that every primitive integral solution $(x,y,z) \in \mathcal{U}(\mathbb{Z})$ *can by obtained by specialization of the parameters* s,t *to values* $s,t \in \mathbb{Z}$*.*

The starting point is the existence of geometrically Galois Belyi maps defined over $\mathbb{Q}$ for the spherical signatures (see Table 3.2). Let $\varphi\colon \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be such a map. For a finite set of rational primes $\mathcal{S}$, we can take an integral model $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ defined over $\mathbb{Z}_{\mathcal{S}}$. Let $G = \operatorname{Aut}(\varphi)$ be the automorphism group scheme. By Theorem 3.5.0.c, we can write $\mathbb{P}^1(a,b,c)\langle \mathbb{Z}_{\mathcal{S}}\rangle$ as the disjoint union of $\varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q}))$, as τ ranges over $\mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, G(\bar{\mathbb{Q}}))$. In particular, we see that for each $(x,y,z) \in \mathcal{U}(\mathbb{Z}) \subset \mathcal{U}(\mathbb{Z}_{\mathcal{S}})$, the point $j(x,y,z) = (-Ax^a : Cz^c)$ is equal to $\varphi_\tau(s:t)$ for a unique τ with the property that $\mathbb{P}^1_\tau \cong \mathbb{P}^1$ (since otherwise $\mathbb{P}^1_\tau(\mathbb{Q}) = \varnothing$), and for some $(s:t) \in \mathbb{P}^1(\mathbb{Q})$. Since each φ_τ is a Galois Belyi map defined over $\mathbb{Q}$, we can find homogeneous polynomials $\Psi_{\tau,0}(\mathsf{s},\mathsf{t}), \Psi_{\tau,1}(\mathsf{s},\mathsf{t})$, and $\Psi_{\tau,\infty}(\mathsf{s},\mathsf{t})$ of degree $\#\bar{\triangle}(a,b,c)$ such that $\varphi_\tau(s:t) = (\Psi_{\tau,0}(s,t) : \Psi_{\tau,\infty}(s,t))$. Moreover,

$$\Psi_{\tau,0}(\mathsf{s},\mathsf{t}) = A_\tau \cdot \mathsf{x}(\mathsf{s},\mathsf{t})^a, \quad \Psi_{\tau,1}(\mathsf{s},\mathsf{t}) = B_\tau \cdot \mathsf{y}(\mathsf{s},\mathsf{t})^b, \quad \Psi_{\tau,\infty}(\mathsf{s},\mathsf{t}) = C_\tau \cdot \mathsf{z}(\mathsf{s},\mathsf{t})^c,$$

where A_τ, B_τ, C_τ are integers supported in $\mathcal{S}$. These are almost the polynomials in the statement of the theorem. To ensure that we hit all of $\mathcal{U}(\mathbb{Z})$ by specializing to $s,t \in \mathbb{Z}$ we must (i) consider the $\mathsf{H}(\mathbb{Z})$-orbits of this polynomials as well, and (ii) apply a suitable change of coordinates. For the second task, Beukers' notices that the set of points $(s,t) \in \mathbb{Q}^2$ such that $(\Psi_{\tau,0}(s,t), \Psi_{\tau,\infty}(s,t)) \in \mathbb{Z}^2$ generates a full lattice $\Lambda_\tau \subset \mathbb{Q}^2$. The change of coordinates in question arises from the choice of an integral basis for Λ_τ. These ideas will be discussed in more detail in Section 4.3.

Chapter 4

Counting primitive integral solutions

4.1 Rational points of bounded height in the image of a rational function

The results presented in this section are undoubtedly well known; however, authors often lose track of the leading constants ([33, p. 133], [19, Theorem B.6.1]. For the sake of completeness, we provide full proofs, making the constants explicit.

Situation 4.1.0.a. Throughout the remainder of this section, we shall work with the following notations.

- Let $\phi\colon \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be a non constant $\mathbb{Q}$-morphism of degree $d := \deg(\phi)$.
- Let $\phi_0, \phi_\infty \in \mathbb{Z}[\mathsf{s}, \mathsf{t}]$ be a choice of relatively prime homogeneous polynomials of degree d such that ϕ is given by

$$\phi(s : t) = (\phi_0(s, t) : \phi_\infty(s, t)).$$

- Let $\mathcal{V} := \mathbb{A}^2 - \mathbf{0}$ be the punctured cone over $\mathbb{P}^1_{\mathbb{Z}}$. We identify $\mathcal{V}(\mathbb{Z})$ with the set $\{(s, t) \in \mathbb{Z}^2 : \gcd(s, t) = 1\}$. The map $\mathcal{V}(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Q})$ given by $(s, t) \mapsto (s : t)$ is two-to-one.

- Denote by $\tilde{\phi}\colon \mathbb{A}^2 \to \mathbb{A}^2$ the lift $\tilde{\phi}(s,t) := (\phi_0(s,t), \phi_\infty(s,t))$ of ϕ.
- On $\mathbb{P}^1(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Z})$, $\mathrm{Ht}\colon \mathbb{P}^1(\mathbb{Q}) \to \mathbb{Z}_{\geqslant 0}$ is the usual multiplicative height, given by $\mathrm{Ht}(Q) = \max\{|\operatorname{num}(Q)|, |\operatorname{den}(Q)|\}$.
- $\Omega(\phi) \subset \mathbb{P}^1(\mathbb{Q})$ is the image of $\phi(\mathbb{Q})\colon \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$.
- For any $\Omega \subset \mathbb{P}^1(\mathbb{Q})$ and for every $h > 0$, $\Omega_{\leqslant h}$ is the finite subset of Ω consisting of those points Q with $\mathrm{Ht}(Q) \leqslant h$. The counting function of $\Omega \subset \mathbb{P}^1(\mathbb{Q})$ is denoted $N(\Omega; h) := \#\Omega_{\leqslant h}$.
- We denote by $\mathrm{Aut}(\phi)$ the group of $\mathbb{Q}$-automorphisms of the map ϕ.

The main result of this section is the following.

Proposition 4.1.0.b. *We have $N(\Omega(\phi); h) \asymp h^{\chi/2}$ as $h \to \infty$. More precisely, there exists an explicitly computable constant $\delta(\phi) > 0$ such that*

$$\delta(\phi) \cdot h^{\chi/2} \leqslant N(\Omega(\phi)); h) \leqslant d \cdot \delta(\phi) \cdot h^{\chi/2}, \qquad \text{as } h \to \infty.$$

The constant $\delta(\phi)$ is described in Equation (4.6)

In the special case where ϕ is geometrically Galois, we can keep track of the exact number of $\mathbb{Q}$-rational points on each fiber $\phi^{-1}(Q) := \mathbb{P}^1 \times_{\mathbb{Q}} Q$, for all but finitely many $Q \in \Omega(\phi)$. This allows us to promote the asymptotic bounds of Proposition 4.1.0.b to an asymptotic count.

Corollary 4.1.0.c. *Suppose that ϕ is geometrically Galois. Then, there exists an explicitly computable constant $\kappa(\phi) \in \mathbb{R}_{>0}$ such that for every $\varepsilon > 0$,*

$$N(\Omega(\phi); h) = \kappa(\phi) \cdot h^{2/d} + O\left(h^{1/d+\varepsilon}\right)$$

as $h \to \infty$. *Moreover, the leading constant is given by*

$$\kappa(\phi) = \delta(\phi)/\#\operatorname{Aut}(\phi),$$

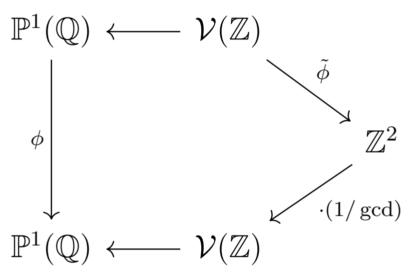
and the implied constant depends on ϕ *and* ε.

4.1.1 The primitivity defect set

Given $(s,t) \in \mathcal{V}(\mathbb{Z})$, it does not follow that $\tilde{\phi}(s,t) = (\phi_0(s,t), \phi_\infty(s,t)) \in \mathcal{V}(\mathbb{Z})$. For example, consider the map

$$\tilde{\phi}(s,t) = ((s^2 - t^2)^2, (2st)^2)$$

arising in the parametrization of Pythagorean triples. When s and t have the same parity, $4 \mid \gcd \tilde{\phi}(s,t)$. In general, $\tilde{\phi}\colon \mathcal{V}(\mathbb{Z}) \to \mathbb{Z}^2$ and we have the following commutative diagram of sets.



Define the primitivity defect set of ϕ by

$$\mathcal{D}(\phi) := \left\{ \gcd \tilde{\phi}(s,t) : (s,t) \in \mathcal{V}(\mathbb{Z}) \right\}. \tag{4.1}$$

The set $\mathcal{D}(\phi)$ is finite. Let $R(\phi) \in \mathbb{Z}$ denote the resultant of the homogeneous polynomials ϕ_0 and ϕ_∞.

Lemma 4.1.1.a. *If* $e \in \mathcal{D}(\phi)$, *then* $e \mid R(\phi)$.

Proof. Let $e \in \mathcal{D}(\phi)$. By definition, there exists $(s,t) \in \mathcal{V}(\mathbb{Z})$ such that $\gcd \tilde{\phi}(s,t) = e$.

In particular, we can find $u, v \in \mathbb{Z}$ such that $u \cdot \phi_0(s,t) + v \cdot \phi_\infty(s,t) = e$. By standard properties of the resultant, we can find polynomials $g_0, g_\infty \in \mathbb{Z}[\mathsf{s},\mathsf{t}]$ such that

$$R(\phi) = g_0(\mathsf{s},\mathsf{t}) \cdot \phi_0(\mathsf{s},\mathsf{t}) + g_\infty(\mathsf{s},\mathsf{t}) \cdot \phi_\infty(\mathsf{s},\mathsf{t}).$$

By evaluating the expression above at $(\mathsf{s},\mathsf{t}) = (s,t)$, we see that $R(\phi)$ is a multiple of e. □

For each $e \in \mathcal{D}(\phi)$, consider the set

$$\mathcal{V}(\mathbb{Z})_e := \left\{ (s,t) \in \mathcal{V}(\mathbb{Z}) : \gcd \tilde{\phi}(s,t) = e \right\}.$$

We have a partition $\mathcal{V}(\mathbb{Z}) = \bigsqcup_{e \in \mathcal{D}(\phi)} \mathcal{V}(\mathbb{Z})_e$.

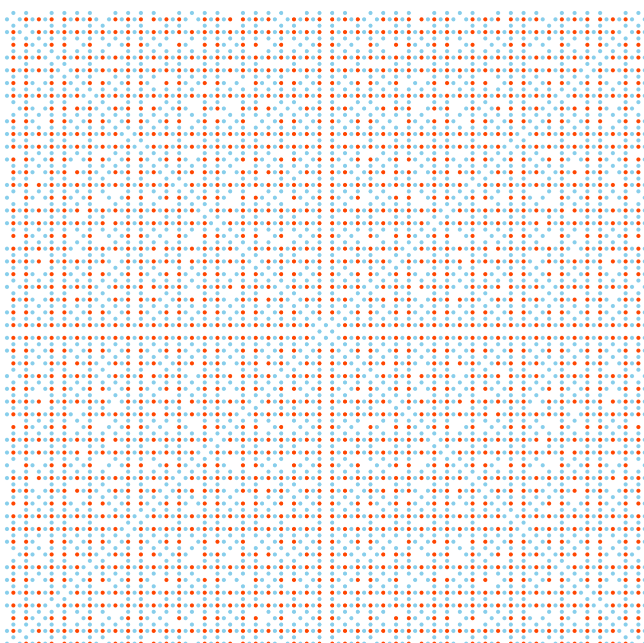


Figure 4.1: Partition $\mathcal{V}(\mathbb{Z}) = \mathcal{V}(\mathbb{Z})_1 \sqcup \mathcal{V}(\mathbb{Z})_4$ with respect to the map $\phi(s:t) = ((s^2 - t^2)^2 : (2st)^2)$, with primitivity defect set $\mathcal{D}(\phi) = \{1, 4\}$.

4.1.2 Proofs

We start with the proof of the asymptotic bounds.

Proof of Proposition 4.1.0.b. For each $e \in \mathcal{D}(\phi)$, consider the lattice

$$\Lambda_e := \mathrm{Span}_{\mathbb{Z}} \mathcal{V}(\mathbb{Z})_e.$$

We will abbreviate $\max \tilde{\phi}(s,t) := \max \{|\phi_0(s,t)|, |\phi_\infty(s,t)|\}$.

Step 1: Lipschitz

We may apply the principle of Lipschitz [14] (in the form of [18, Lemma 2.22]) to obtain

$$\begin{aligned} \widetilde{N}_e(h) &:= \# \left\{ (s,t) \in \Lambda_e : \max \tilde{\phi}(s,t) \leqslant eh \right\} \\ &= \delta(\phi, e) \cdot h^{2/d} + O_e\left(h^{1/d}\right). \end{aligned} \tag{4.2}$$

The constant is given by

$$\delta(\phi, e) = \frac{\sqrt[d]{e} \cdot \mathrm{vol}\left(\mathcal{R}(\phi, 1)\right)}{\det \Lambda_e},$$

where $\mathrm{vol}\left(\mathcal{R}(\phi,1)\right)$ is the Lebesgue measure of the compact region $\mathcal{R}(\phi,1)$ in $\mathbb{R}^2$ given by $\max\{|\phi_0(s,t)|, |\phi_\infty(s,t)|\} \leqslant 1$, and $\det \Lambda_e$ is the covolume of the lattice Λ_e.

Step 2: Möbius sieving

We intersect Λ_e with $\mathcal{V}(\mathbb{Z})$ and apply a standard Möbius sieve to Equation (4.2) to obtain, for every $\varepsilon > 0$, the asymptotic

$$\begin{aligned} N_e(h) &:= \#\left\{(s,t) \in \mathcal{V}(\mathbb{Z})_e : \max \tilde{\phi}(s,t) \leqslant eh\right\} \\ &= \frac{6}{\pi^2} \cdot \delta(e) \cdot h^{2/d} + O_{e,\varepsilon}\left(h^{1/d+\varepsilon}\right). \end{aligned} \tag{4.3}$$

Indeed, from the partition

$$\begin{aligned} &\left\{(s,t) \in \Lambda_e : \max \tilde{\phi}(s,t) \leqslant eh\right\} = \\ &\bigsqcup_{1 \leqslant m \leqslant \sqrt[d]{eh}} \left\{(ms,mt) \in \Lambda_e : m^d \max \tilde{\phi}(s,t) \leqslant eh, \ \ \gcd(s,t) = e\right\}, \end{aligned}$$

we deduce that

$$\widetilde{N}_e(h) = \sum_{1 \leqslant m \leqslant \sqrt[d]{eh}} N_e(h/m^d).$$

From Möbius inversion (see [3, Theorem 2.23]), we get

$$\begin{aligned} N_e(h) &= \sum_{1 \leqslant m \leqslant \sqrt[d]{eh}} \mu(m) \widetilde{N}_e(h/m^d) \\ &= \sum_{1 \leqslant m \leqslant \sqrt[d]{eh}} \mu(m) \left(\frac{\delta(\phi,e)}{m^2} \cdot h^{2/d} + O_e\left(\frac{h^{1/d}}{m}\right)\right) \\ &= \sum_{1 \leqslant m \leqslant \sqrt[d]{eh}} \mu(m) \cdot \delta(\phi,e) \cdot \frac{h^{2/d}}{m^2} + \sum_{1 \leqslant m \leqslant \sqrt[d]{eh}} O_e\left(\frac{h^{1/d}}{m}\right) \\ &= \delta(\phi,e) \cdot h^{2/d} \sum_{1 \leqslant m \leqslant \sqrt[d]{eh}} \frac{\mu(m)}{m^2} + h^{1/d} O_e\left(\sum_{1 \leqslant m \leqslant \sqrt[d]{eh}} \frac{1}{m^{\varepsilon}}\right). \end{aligned}$$

From this last expression we see that Equation (4.3) holds as $h \to \infty$.

Step 3: back to $\mathbb{P}^1(\mathbb{Q})$.

Consider the related counting function

$$N_\phi(h) := \#\left\{(s:t) \in \mathbb{P}^1(\mathbb{Q}) : \mathrm{Ht}(\phi(s:t)) \leqslant h\right\},$$

which counts all $\mathbb{Q}$-rational points on $\mathbb{P}^1$ with respect to the height Ht pulled back by ϕ. In general, we have the inequalities

$$N(\Omega(\phi); h) \leqslant N_\phi(h) \leqslant d \cdot N(\Omega(\phi); h) \tag{4.4}$$

which arise from the fact that a point $Q = \phi(P) \in \Omega(\phi)$ has at least one rational point in the fiber $\phi^{-1}(Q)$, and at most $d = \deg \phi$.

To conclude, we relate $N_\phi(h)$ to the previous estimates.

$$\begin{aligned} N_\phi(h) &= \frac{1}{2} \sum_{e \in \mathcal{D}(\phi)} N_e(h) \\ &= \frac{1}{2} \sum_{e \in \mathcal{D}(\phi)} \frac{6}{\pi^2} \cdot \delta(\phi, e) \cdot h^{2/d} + O\left(h^{1/d+\varepsilon}\right). \\ &= \frac{3}{\pi^2} \left(\sum_{e \in \mathcal{D}(\phi)} \delta(\phi, e) \right) \cdot h^{2/d} + O\left(h^{1/d+\varepsilon}\right). \end{aligned} \tag{4.5}$$

In particular, the constant term is

$$\delta(\phi) = \frac{3}{\pi^2} \sum_{e \in \mathcal{D}(\phi)} \delta(\phi, e). \tag{4.6}$$

□

We will use Proposition 4.1.0.b in the special case of a geometrically Galois $\mathbb{Q}$-Belyi map ϕ.

Proof of Corollary 4.1.0.c. Suppose that ϕ is geometrically Galois, with Galois group

$\mathrm{Gal}(\phi) = \mathrm{Aut}(\phi_{\bar{\mathbb{Q}}})$. Then, $\mathrm{Gal}(\phi)$ acts transitively and without stabilizers on the fibers of unramified points $Q \in \mathbb{P}^1(\mathbb{Q})$. Since there are finitely many points that ramify, they do not influence the asymptotic count, so we ignore them. We claim that for every $Q \in \phi(\mathbb{P}^1(\mathbb{Q})) = \Omega(\phi)$, we have that

$$\#\phi^{-1}(Q)(\mathbb{Q}) = \#\,\mathrm{Aut}(\phi).$$

Indeed $\mathrm{Aut}(\phi) = \mathrm{Aut}(\phi_{\bar{\mathbb{Q}}})^{\mathrm{Gal}_{\bar{\mathbb{Q}}}}$, and for every $P \in \phi^{-1}(Q)(\mathbb{Q})$ and $\gamma \in \mathrm{Aut}(\phi)$, we have that $\gamma(P) \in \phi^{-1}(Q)(\mathbb{Q})$ as well. On the other hand, given $P, P' \in \phi^{-1}(Q)(\mathbb{Q})$, there exists $\gamma \in \mathrm{Aut}(\phi_{\bar{\mathbb{Q}}})$ such that $\gamma(P') = P$. For any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, we see that $\gamma^\sigma(P') = \gamma(\sigma^{-1}P') = \gamma(P')$. Therefore, $\gamma^{-1}\gamma^\sigma$ stabilizes P', which implies that $\gamma^{-1}\gamma^\sigma = 1$, and therefore $\gamma \in \mathrm{Aut}(\phi)$. It follows that $N_\phi(h) = \#\,\mathrm{Aut}(\phi) \cdot N(\Omega(\phi); h)$, and the proof is complete. □

4.2 Counting integral points on the Belyi stack

Situation 4.2.0.a (Counting integral points on the Belyi stack)**.** Here

- Let $\mathbf{e} = (a, b, c)$ be a spherical signature (see Table 3.1), with $a, b, c > 1$.
- Let $\mathbb{P}^1(a, b, c)$ be the Belyi stack of signature (a, b, c).
- Let $\mathcal{S}$ is a finite set of primes containing all prime divisors of $a \cdot b \cdot c$.
- Let $\mathbb{Z}_{\mathcal{S}}$ be the ring of $\mathcal{S}$-integers.
- Recall that $\mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, \bullet)$ denotes the Galois cohomology set classifying $\bullet$-torsors over $\operatorname{Spec}\mathbb{Q}$ unramified outside of $\mathcal{S}$.
- Let $\Omega(\mathbf{e}, \mathcal{S}) \subset \mathbb{P}^1(\mathbb{Q})$ be the set of $\mathbb{Z}_{\mathcal{S}}$-points on $\mathbb{P}^1(a, b, c)$. See Lemma 3.1.3.d.
- For any $\Omega \subset \mathbb{P}^1(\mathbb{Q})$, and any $h > 0$, we have the counting function $N(\Omega; h)$ defined in Situation 4.1.0.a.

The main result of this section is the asymptotic order of growth of the counting function $N(\Omega(\mathbf{e}, \mathcal{S}); h)$.

Theorem 4.2.0.b. *There exists an explicitly computable constant $\kappa(\mathbf{e}, \mathcal{S}) > 0$ such that, for every $\varepsilon > 0$*

$$N(\Omega(a, b, c), h) = \kappa(\mathbf{e}, \mathcal{S}) \cdot h^{\chi} + O(h^{\chi/2+\varepsilon}),$$

as $h \to \infty$. The implicit constant depends on $\mathbf{e}$, $\mathcal{S}$, and ε.

Proof. We argue as in Section 3.5.2. It is well known that for every spherical signature there exists a geometrically Galois Belyi map $\varphi_{\mathbb{Q}}$ defined over $\mathbb{Q}$. Moreover, these maps admit integral models $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ over $\mathbb{Z}_{\mathcal{S}}$. The map φ gives rise to an fppf $\operatorname{Aut}(\varphi)$-torsor $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1(a, b, c)$, defined over $\operatorname{Spec} \mathbb{Z}_{\mathcal{S}}$. In particular, $\mathbb{P}^1(a, b, c) \cong [\mathbb{P}^1 / \operatorname{Aut}(\varphi)]$ over $\operatorname{Spec} \mathbb{Z}_{\mathcal{S}}$. By descent, we have that

$$\mathbb{P}^1(a, b, c)\langle R\rangle = \bigsqcup_{\tau \in \mathrm{H}^1(R, \operatorname{Aut}(\varphi_R))} \varphi_\tau(\mathbb{P}^1_\tau(R)) = \bigsqcup_{\tau \in \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, G)} \varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).$$

We conclude that $N(\Omega(\mathbf{e}, \mathcal{S}); h)$ is the sum of $N(\Omega(\varphi_\tau); h)$ where τ ranges over those cohomology classes in $\mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, G)$ such that $\mathbb{P}^1_\tau(\mathbb{Q}) \neq \varnothing$. Since for every such τ, the twists $\varphi_\tau\colon \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ are geometrically Galois Belyi maps defined over $\mathbb{Q}$, the result follows by Corollary 4.1.0.c. □

4.3 Counting primitive integral solutions to generalized Fermat equations

Situation 4.3.0.a (Counting primitive integer solutions)**.** Here

- Let $F\colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0$ be a spherical generalized Fermat equation with integer coefficients.

- Let $\mathcal{U}$ be the punctured cone over $\mathbb{Z}$ associated to F, as in Definition 3.2.1.b.
- Let G denote the triangle group $\bar{\Delta}(a,b,c)$, defined in Definition 3.1.1.a.
- Let $\mathcal{S}$ be the set of rational primes p dividing $a \cdot b \cdot c$ or $A \cdot B \cdot C$.
- Let $\mathbb{Z}_{\mathcal{S}}$ be the ring of $\mathcal{S}$-integers.

Theorem 4.3.0.b. *Consider Equation (1.1) with $A, B, C \in \mathbb{Z}^3$ nonzero and $a, b, c > 1$. Suppose that $\chi := \chi(a,b,c) > 0$, and that there exists at least one primitive integral solution to F. Then, there exists an explicit constant $\kappa(F) > 0$ such that for every $\varepsilon > 0$,*

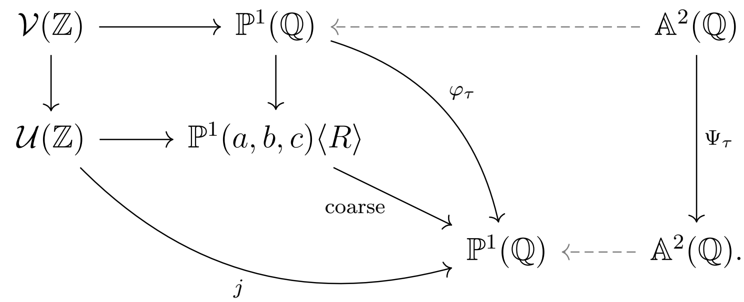
$$N(\Omega(F), h) = \kappa(F) \cdot h^{\chi} + O(h^{\chi/2+\varepsilon}),$$

as $h \to \infty$. The implied constant depends on F and ε.

Proof. Without loss of generality, we assume that $\gcd(A,B,C) = 1$. We work over $R = \mathbb{Z}_{\mathcal{S}}$. Our starting point is as in the proof of Theorem 4.2.0.b. Let G denote the automorphism group scheme of a Galois Belyi map $\varphi \colon \mathbb{P}^1 \to \mathbb{P}^1$ of signature (a,b,c), defined over $\operatorname{Spec} \mathbb{Z}_{\mathcal{S}}$. We have the partition

$$\mathbb{P}^1(a,b,c)\langle \mathbb{Z}_{\mathcal{S}} \rangle = \bigsqcup_{\tau \in \mathrm{H}^1(\mathbb{Z}_{\mathcal{S}}, G)} \varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Z}_{\mathcal{S}})) = \bigsqcup_{\tau \in \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, G(\bar{\mathbb{Q}}))} \varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).$$

Recal that the j-map $j \colon \mathcal{U} \to \mathbb{P}^1$ is given by $(x,y,z) \mapsto (-Ax^a : Cz^c)$. Noting that $j(\mathcal{U}(\mathbb{Z})) \subset \mathbb{P}^1(a,b,c)\langle R \rangle = \Omega(\mathbf{e}, \mathcal{S})$, we define $\mathrm{T}_F \subset \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, G(\bar{\mathbb{Q}}))$ to be the subset of those cohomology classes τ such that $j(\mathcal{U}(\mathbb{Z})) \cap \varphi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})) \neq \varnothing$. Observe that $\mathcal{U}(\mathbb{Z}) \neq \varnothing$ implies that $\mathrm{T}_F \neq \varnothing$. Moreover, for every $\tau \in \mathrm{T}_F$ we have that $(\mathbb{P}^1_\tau)_{\mathbb{Q}} \cong \mathbb{P}^1_{\mathbb{Q}}$. Each map $\varphi_\tau \colon \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ is descends from a map $\Psi_\tau \colon \mathbb{A}^2_{\mathbb{Q}} \to \mathbb{A}^2_{\mathbb{Q}}$. For each $\tau \in \mathrm{T}_F$ we have a commutative diagram of sets



(4.7)

Explicitly, $\Psi_\tau = (\Psi_{\tau,0}, \Psi_{\tau,\infty})$ where $\Psi_{\tau,0}, \Psi_{\tau,\infty} \in \mathbb{Z}[\mathsf{s},\mathsf{t}]$ are homogeneous polynomials of degree $\#G(\bar{\mathbb{Q}}) = \#\bar{\triangle}(a,b,c)$ satisfying the following two conditions:

(i) $\Psi_{\tau,0}/\Psi_{\tau,\infty} = 1 + \Psi_{\tau,1}/\Psi_{\tau,\infty}$ for some $\Psi_{\tau,1} \in \mathbb{Z}[\mathsf{s},\mathsf{t}]$ homogeneous of the same degree.

(ii) The ideals generated by these polynomials in $R[\mathsf{s},\mathsf{t}]$ are perfect (a,b,c) powers. More precisely: $\Psi_{\tau,0}R[\mathsf{s},\mathsf{t}] = J_0^a, \Psi_{\tau,1}R[\mathsf{s},\mathsf{t}] = J_1^b$, and $\Psi_{\tau,\infty}R[\mathsf{s},\mathsf{t}] = J_\infty^c$ for nonzero principal ideals $J_0, J_1, J_\infty \subset R[\mathsf{s},\mathsf{t}]$.

Following Beukers [7, Proof of Theorem 1.5], for each $\tau \in \mathrm{T}_F$ we consider the full lattice $\Lambda_\tau \subset \mathbb{Q}^2 = \mathbb{A}^2(\mathbb{Q})$ defined as the $\mathbb{Z}$-span of those pairs $(s,t) \in \mathbb{Q}^2$ such that $\Psi_\tau(s,t) \in \mathbb{Z}^2$. Chose integral bases $\left\{\vec{\alpha}_\tau, \vec{\beta}_\tau\right\}$ for each Λ_τ and consider the rational function

$$f_\tau(\mathsf{s},\mathsf{t}) := \frac{\Psi_{\tau,0}(\mathsf{s}\vec{\alpha}_\tau + \mathsf{t}\vec{\beta}_\tau)}{\Psi_{\tau,\infty}(\mathsf{s}\vec{\alpha}_\tau + \mathsf{t}\vec{\beta}_\tau)} = 1 + \frac{\Psi_{\tau,1}(\mathsf{s}\vec{\alpha}_\tau + \mathsf{t}\vec{\beta}_\tau)}{\Psi_{\tau,\infty}(\mathsf{s}\vec{\alpha}_\tau + \mathsf{t}\vec{\beta}_\tau)}.$$

By construction, we have the partition

$$j(\mathcal{U}(\mathbb{Z})) = \bigsqcup_{\tau \in \mathrm{T}_F} f_\tau(\mathbb{P}^1(\mathbb{Q})).$$

The result now follows from Corollary 4.1.0.c. □

Bibliography

[1] Dan Abramovich and Brendan Hassett. Stable varieties with a twist. In *Classification of algebraic varieties*, EMS Ser. Congr. Rep., pages 1–38. Eur. Math. Soc., Zürich, 2011. ISBN 978-3-03719-007-4. doi: 10.4171/007-1/1. URL https://doi.org/10.4171/007-1/1.

[2] Jarod Alper. Good moduli spaces for Artin stacks. *Ann. Inst. Fourier (Grenoble)*, 63(6):2349–2402, 2013. ISSN 0373-0956,1777-5310. doi: 10.5802/aif.2833. URL https://doi.org/10.5802/aif.2833.

[3] Tom M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[4] Kai Behrend and Behrang Noohi. Uniformization of Deligne-Mumford curves. *J. Reine Angew. Math.*, 599:111–153, 2006. ISSN 0075-4102,1435-5345. doi: 10.1515/CRELLE.2006.080. URL https://doi.org/10.1515/CRELLE.2006.080.

[5] G. V. Belyi. Galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(2):267–276, 479, 1979. ISSN 0373-2436.

[6] G. V. Belyi. A new proof of the three-point theorem. *Mat. Sb.*, 193(3):21–24, 2002. ISSN 0368-8666,2305-2783. doi: 10.1070/SM2002v193n03ABEH000633. URL https://doi.org/10.1070/SM2002v193n03ABEH000633.

[7] Frits Beukers. The Diophantine equation $Ax^p+By^q = Cz^r$. *Duke Math. J.*, 91(1):

61–88, 1998. ISSN 0012-7094,1547-7398. doi: 10.1215/S0012-7094-98-09105-0. URL https://doi.org/10.1215/S0012-7094-98-09105-0.

[8] Pete L. Clark and John Voight. Algebraic curves uniformized by congruence subgroups of triangle groups. *Trans. Amer. Math. Soc.*, 371(1):33–82, 2019. ISSN 0002-9947,1088-6850. doi: 10.1090/tran/7139. URL https://doi.org/10.1090/tran/7139.

[9] Henri Cohen. *Number theory. Vol. II. Analytic and modern tools*, volume 240 of *Graduate Texts in Mathematics*. Springer, New York, 2007. ISBN 978-0-387-49893-5.

[10] Brian Conrad. The Keel–Mori theorem via stacks. Available at https://math.stanford.edu/~conrad/papers/coarsespace.pdf, November 2005.

[11] Brian Conrad. Reductive group schemes. In *Autour des schémas en groupes. Vol. I*, volume 42/43 of *Panor. Synthèses*, pages 93–444. Soc. Math. France, Paris, 2014. ISBN 978-2-85629-794-0.

[12] H. Darmon. Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation. *C. R. Math. Rep. Acad. Sci. Canada*, 19(1):3–14, 1997. ISSN 0706-1994.

[13] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995. ISSN 0024-6093,1469-2120. doi: 10.1112/blms/27.6.513. URL https://doi.org/10.1112/blms/27.6.513.

[14] H. Davenport. On a principle of Lipschitz. *J. London Math. Soc.*, 26:179–183, 1951. ISSN 0024-6107,1469-7750. doi: 10.1112/jlms/s1-26.3.179. URL https://doi.org/10.1112/jlms/s1-26.3.179.

[15] Johnny Edwards. A complete solution to $X^2 + Y^3 + Z^5 = 0$. *J. Reine Angew. Math.*, 571:213–236, 2004. ISSN 0075-4102,1435-5345. doi: 10.1515/crll.2004.043. URL https://doi.org/10.1515/crll.2004.043.

[16] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. ISSN 0020-9910,1432-1297. doi: 10.1007/BF01388432. URL https://doi.org/10.1007/BF01388432.

[17] Alexander Grothendieck. Éléments de géométrie algébrique : II. étude globale élémentaire de quelques classes de morphismes. *Publications Mathématiques de l'IHÉS*, 8:5–222, 1961. URL https://www.numdam.org/item/PMIHES_1961__8__5_0/.

[18] D. R. Heath-Brown and Daniel Loughran. Manin's conjecture for quintic del Pezzo surfaces with a conic bundle structure. *arXiv e-prints*, art. arXiv:2506.02829, June 2025. doi: 10.48550/arXiv.2506.02829.

[19] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. ISBN 0-387-98975-7; 0-387-98981-1. doi: 10.1007/978-1-4612-1210-2. URL https://doi.org/10.1007/978-1-4612-1210-2. An introduction.

[20] J. Lambek and L. Moser. On the distribution of Pythagorean triangles. *Pacific J. Math.*, 5:73–83, 1955. ISSN 0030-8730. URL http://projecteuclid.org/euclid.pjm/1103044610.

[21] Derrick Norman Lehmer. Asymptotic Evaluation of Certain Totient Sums. *Amer. J. Math.*, 22(4):293–335, 1900. ISSN 0002-9327,1080-6377. doi: 10.2307/2369728. URL https://doi.org/10.2307/2369728.

[22] Wilhelm Magnus. *Noneuclidean tesselations and their groups*, volume Vol. 61

of *Pure and Applied Mathematics*. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1974.

[23] James S. Milne. *Étale cohomology*, volume No. 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1980. ISBN 0-691-08238-3.

[24] Joseph Oesterlé. Schémas en groupes de type multiplicatif. In *Autour des schémas en groupes. Vol. I*, volume 42/43 of *Panor. Synthèses*, pages 63–91. Soc. Math. France, Paris, 2014. ISBN 978-2-85629-794-0.

[25] Martin Olsson. *Algebraic spaces and stacks*, volume 62 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2016. ISBN 978-1-4704-2798-6. doi: 10.1090/coll/062. URL https://doi.org/10.1090/coll/062.

[26] Bjorn Poonen. Unramified covers of Galois covers of low genus curves. *Math. Res. Lett.*, 12(4):475–481, 2005. ISSN 1073-2780. doi: 10.4310/MRL.2005.v12.n4.a3. URL https://doi.org/10.4310/MRL.2005.v12.n4.a3.

[27] Bjorn Poonen. The projective line minus three fractional points. Slides for the MSRI program: Rational and integral points on higher-dimensional varieties, July 2006.

[28] Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017. ISBN 978-1-4704-3773-2. doi: 10.1090/gsm/186. URL https://doi.org/10.1090/gsm/186.

[29] Bjorn Poonen. Some examples of stacks. Slides for the AMS MRC: Explicit computations with stacks, June 2023.

[30] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll. Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$. *Duke Math. J.*, 137(1):103–158, 2007. ISSN 0012-7094,1547-7398. doi: 10.1215/S0012-7094-07-13714-1. URL https://doi.org/10.1215/S0012-7094-07-13714-1.

[31] Tim Santens. The Brauer-Manin obstruction for stacky curves. *arXiv e-prints*, art. arXiv:2210.17184v3, October 2022. doi: 10.48550/arXiv.2210.17184v3.

[32] Tim Santens. Quantitative arithmetic and the Brauer group, 2024.

[33] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. ISBN 3-528-28968-6. doi: 10.1007/978-3-663-10632-6. URL https://doi.org/10.1007/978-3-663-10632-6. With a foreword by Brown and Serre.

[34] Alexei Skorobogatov. *Torsors and rational points*, volume 144 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2001. ISBN 0-521-80237-7. doi: 10.1017/CBO9780511549588. URL https://doi.org/10.1017/CBO9780511549588.

[35] The Stacks project authors. The stacks project. https://stacks.math.columbia.edu, 2024.

[36] Richard P. Stanley. Smith normal form in combinatorics. *J. Combin. Theory Ser. A*, 144:476–495, 2016. ISSN 0097-3165,1096-0899. doi: 10.1016/j.jcta.2016.06.013. URL https://doi.org/10.1016/j.jcta.2016.06.013.

[37] Ravi Vakil. The rising sea: foundations of algebraic geometry, April 2023.

[38] John Voight and David Zureick-Brown. The canonical ring of a stacky curve. *Mem. Amer. Math. Soc.*, 277(1362):v+144, 2022. ISSN 0065-9266,1947-6221. doi: 10.1090/memo/1362. URL https://doi.org/10.1090/memo/1362.