COUNTING PRIMITIVE INTEGRAL SOLUTIONS TO SPHERICAL GENERALIZED FERMAT EQUATIONS

SANTIAGO ARANGO-PIÑEROS

ABSTRACT. A solution $(x, y, z) \in \mathbb{Z}^3 - \{(0, 0, 0)\}$ to a generalized Fermat equation

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

is called *primitive* if $\gcd(x, y, z) = 1$. By work of Beukers [Beu98], we know that in the *spherical* regime (that is, when the Euler characteristic $\chi = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$ is positive), if Equation (1) has one primitive solution, then it has infinitely many. In this work, we use the method of *Fermat descent*, as employed by Poonen–Schaefer-Stoll [PSS07], to refine Beukers' result to an asymptotic count of the number of primitive integral solutions of bounded height.

MSC class: 11D41

CONTENTS

1. INTRODUCTION

1.1. **Poonen's heuristic.** We follow [Poo06]. Let a, b, c be positive integers, and consider the following subset of the rational points on the projective line $\mathbb{P}^1(\mathbb{Q}) \cong \mathbb{Q} \cup \left\{\frac{1}{0}\right\}$.

$$\Omega(a, b, c) := \left\{ Q \in \mathbb{P}^1(\mathbb{Q}) : \begin{array}{l} \text{(i) } \operatorname{num}(Q) \text{ is an } a^{\text{th}} \text{ power,} \\ \text{(ii) } \operatorname{num}(Q-1) \text{ is a } b^{\text{th}} \text{ power,} \\ \text{(iii) } \operatorname{den}(Q) \text{ is a } c^{\text{th}} \text{ power.} \end{array} \right\}. \tag{2}$$

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 $\pm(s, t) \in \mathbb{Z}^2$ for $Q = (s : t)$ with $\gcd(s, t) = 1$. 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

$$\Omega_{\leqslant h} := \{Q \in \Omega : \mathrm{Ht}(Q) \leqslant h\}, \quad N(\Omega; h) := \#\Omega_{\leqslant h}, \tag{3}$$

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

$$\mathrm{Ht}(Q) = \max\{|\operatorname{num}(Q)|, |\operatorname{den}(Q)|\}. \tag{4}$$

Heuristic 1.1. 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 (2) 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

$$\chi(a,b,c) := \tfrac{1}{a} + \tfrac{1}{b} + \tfrac{1}{c} - 1 \tag{5}$$

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 [DG95, Theorem 2]. The spherical case (when $\chi > 0$) can be deduced from a theorem of Beukers [Beu98, Theorem 1.2]. More precisely, the heuristic suggests that in the spherical case one has $N(\Omega(a,b,c); h) \asymp h^{\chi}$, as h tends to infinity.

1.2. **Results.** Our first result confirms the prediction of Heuristic 1.1.

Theorem 1.2. *Suppose that $a, b, c > 1$ and that $\chi := \chi(a, b, c) > 0$. Then, there exists an explicitly computable constant $\kappa(a, b, c) > 0$ such that for every $\varepsilon > 0$,*

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

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

Consider the generalized Fermat equation

$$F\colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^d = 0 \subset \mathbb{A}^3_{\mathbb{Z}} \tag{6}$$

for arbitrary integers A, B, C satisfying $A \cdot B \cdot C \neq 0$. A solution $(x, y, z) \in \mathbb{Z}^3 - \{(0, 0, 0)\}$ is said to be primitive when $\gcd(x, y, z) = 1$. Corresponding to each F, we have the punctured cone $\mathcal{U}$ (obtained by deleting the closed subscheme $\{\mathsf{x} = \mathsf{y} = \mathsf{z} = 0\}$ from F) and the morphism

$$j\colon \mathcal{U} \to \mathbb{P}^1_{\mathbb{Z}}, \quad (x, y, z) \mapsto (-Ax^a : Cz^c). \tag{7}$$

Note that $\mathcal{U}(\mathbb{Z})$ is identified with the set of primitive integral solutions to F. Define the subset $\Omega(F) \subset \mathbb{P}^1(\mathbb{Q})$ to be the image of the function $j(\mathbb{Z})\colon \mathcal{U}(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Z}) = \mathbb{P}^1(\mathbb{Q})$.

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 (6) for some choice of $(A, B, C) \in \{\pm 1\}^3$. 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 $Q = \pm x^a/z^c$ is in $\Omega(a, b, c)$.

By carefully identifying how the sets $\Omega(F)$ fit inside of $\Omega(a, b, c)$ (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 1.3. *Consider Equation (6) with $A, B, C \in \mathbb{Z}$ 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 ε.

1.3. $\mathcal{S}$-integral points on the Belyi stack.

Our approach is geometric. We use the method of *Fermat descent*, developed by [DG95], [Dar97], and [PSS07], and expanded on in [AP25] from the point of view of stacks. It turns out $\Omega(a,b,c)$ is precisely the set of $\mathbb{Z}$-points on the Belyi stack of signature (a,b,c), denoted by $\mathbb{P}^1(a,b,c)$ (see [AP25, Section 3]). This is the stacky version of Darmon's M-curve $\mathbf{P}^1_{a,b,c}$ [Dar97, p. 4].

Notation 1.4 (Set of points on a stack)**.** If $\mathcal{X}$ is a stack and R is a ring, we denote by $\mathcal{X}(R)$ the *groupoid* of R-points, and by $\mathcal{X}\langle R\rangle$ the *set* of R-points, (see [AP25, Section 2.1]).

For the purposes of this work, we need only to understand the set $\mathbb{P}^1(a,b,c)\langle R\rangle$ in the case that $R = \mathbb{Z}[\mathcal{S}^{-1}]$ for some finite set of rational primes $\mathcal{S}$. In [AP25, Lemma 3.3], we show that the set $\mathbb{P}^1(a,b,c)\langle R\rangle$ is in bijective correspondence with the subset $\Omega_{\mathcal{S}}(a,b,c)$ of the rational points on the projective line of points $Q \in \mathbb{P}^1(\mathbb{Q})$ which satisfy the property that the ideals

$$\operatorname{num}(Q)R, \quad \operatorname{num}(Q-1)R, \quad \operatorname{den}(Q)R, \tag{8}$$

are a^{th}, b^{th}, and c^{th} powers respectively. Since R is a principal ideal domain, Q belongs to $\Omega_{\mathcal{S}}(a,b,c) \subset \mathbb{P}^1(\mathbb{Q})$ if and only if

$$\operatorname{num}(Q) = -Ax^a, \quad \operatorname{num}(Q-1) = By^b, \quad \operatorname{den}(Q) = Cz^c,$$

for some $A,B,C \in R^\times$, and $x,y,z \in \mathbb{Z}$ with $\gcd(x,y,z) = 1$. This choice of coefficients $(A,B,C) \in (R^\times)^3$ is only well defined up to coordinate-wise multiplication by a unit in R. In particular, we can arrange for A,B,C to be in $\mathbb{Z} \cap R^\times = \{n \in \mathbb{Z} : p \mid n \text{ implies } p \in \mathcal{S}\}$. These considerations lead to the following definition.

Definition 1.5. Let $\mathcal{S}$ be a finite set of primes. Define the $\mathcal{S}$-simplified Fermat coefficient triple of a point $Q \in \Omega_{\mathcal{S}}(a,b,c)$ to be the unique triple $(A,B,C) \in \mathbb{Z}^3$ satisfying the following properties:

(i) The integers A,B,C are $\mathcal{S}$-units.
(ii) A is a^{th} power-free, B is b^{th} power-free, and C is c^{th} power-free.
(iii) $A > 0$.
(iv) $A \mid \operatorname{num}(Q)$, $B \mid \operatorname{num}(Q-1)$, and $C \mid \operatorname{den}(Q)$.

We denote this assignment by $\mathbf{sfc}(Q) = (A,B,C)$. We say that a generalized Fermat equation $F\colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0$ is $\mathcal{S}$-simple or $\mathcal{S}$-simplified if the coefficients (A,B,C) satisfy the properties (i), (ii), and (iii) above. We say that F is simple or simplified, if it is $\mathcal{S}$-simple for $\mathcal{S} := \{p \text{ prime} : p \mid A \cdot B \cdot C\}$.

Example 1.6. The $\varnothing$-simple Fermat equations have ±1 coefficients.

1.4. **The Pythagorean case.** To introduce the main ideas in our proofs, we consider the elementary case of signature $(a, b, c) = (2, 2, 2)$, where the mention of stacks is unnecessary and could be considered excessive. We remark that Lehmer [Leh00, p. 38] and Lambek–Moser [LM55] already counted the number of Pythagorean triangles with bounded hypotenuse, and the analytic number theory techniques used in their work and in ours remain essentially the same. In our notation, their theorem would read as follows.

Theorem 1.7 (Lehmer, Lambek–Moser)**.** *Consider the Pythagorean equation* $F_3\colon \mathsf{x}^2 + \mathsf{y}^2 - \mathsf{z}^2 = 0$. *Then,*

$$N(\Omega(F_3); h) \sim \tfrac{1}{\pi} \cdot h^{1/2},$$

as $h \to \infty$*.*

Our first observation is that Theorem 1.7 implies the special case of Theorem 1.2 for signature $(a, b, c) = (2, 2, 2)$.

Theorem 1.8. *The asymptotic*

$$N(\Omega(2, 2, 2); h) \sim \tfrac{3}{\pi} \cdot h^{1/2}$$

holds, as $h \to \infty$*.*

Proof. Consider the group $G := \{\pm 1\}^3 / \pm 1$, and list its elements

$$e_0 = [1, 1, 1], \quad e_1 = [-1, 1, 1], \quad e_2 = [1, -1, 1], \quad e_3 = [1, 1, -1].$$

Consider the Fermat conics F_0, F_1, F_2, F_3 with $\mathsf{x}^2, \mathsf{y}^2, \mathsf{z}^2$ coefficients given by the element in G with matching index. For each element in G, we attach a corresponding map $j\colon \mathcal{U} \to \mathbb{P}^1$ as in Equation (7).

Table 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	$\mathsf{x}^2 + \mathsf{y}^2 - \mathsf{z}^2 = 0$	$(x, y, z) \mapsto (x^2 : z^2)$

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 pairwise intersections $\Omega(F_i)\cap\Omega(F_j)$ for $i,j\in\{1,2,3\}$ are contained in $\{0,1,\infty\}$. This can be checked by partitioning the set $\Omega(2,2,2)$ according to the signs of $\operatorname{num}(Q)$, $\operatorname{num}(Q-1)$, and $\operatorname{den}(Q)$, and staring at Table 1. From this description, we deduce that

$$N(\Omega(2,2,2);h)=N(\Omega(F_1);h)+N(\Omega(F_2);h)+N(\Omega(F_3);h)\sim\tfrac{12}{\pi}\cdot h^{1/2}.$$

□

Now, we will prove Theorem 1.7 using the method of *Fermat descent*.

Proof of Theorem 1.7. The proof proceeds in three steps: covering, twisting, and sieving.

Step 1: (Covering) A suitable covering is readily available. Indeed, if 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

$$\phi_0\colon Z_0\to\mathbb{P}^1_{\mathbb{Q}},\quad (x:y:z)\mapsto(-x^2:z^2).$$

One verifies that ϕ is a Galois Belyi map defined over $\mathbb{Q}$ with Galois group G, diagonally embedded in $\mathrm{PGL}_3(\mathbb{Q})$. Since $\mathcal{U}_0(\mathbb{Z})$ is empty, so is $\Omega(F_0)$.

Any other cover $\phi_i\colon Z_i\to\mathbb{P}^1$ (induced from $j_i\colon\mathcal{U}_i\to\mathbb{P}^1$) would suffice, but we choose the pointless conic for dramatic emphasis.

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

The only bad prime for the covering (in the sense of [AP25, Lemma 3.23]) ϕ is $p=2$. In the notation of Section 1.3, $\mathcal{S}=\{2\}$, and $R=\mathbb{Z}[1/2]$. By descent theory, we are only interested in the subset $\mathrm{H}^1_{\mathcal{S}}(\mathbb{Q},G)\subset\mathrm{H}^1(\mathbb{Q},G)$ corresponding to those injections $\mathrm{Gal}(L|\mathbb{Q})\hookrightarrow G$ for which L is unramified outside $\{2\}$. The possible fields are

$$L\in\left\{\mathbb{Q},\mathbb{Q}(\sqrt{-1}),\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{-2}),\mathbb{Q}(\zeta_8)\right\}.$$

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

$$\Omega_{\mathcal{S}}(2,2,2) = \bigsqcup_{\rho \in \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q},G)} \phi_\rho(Z_\rho(\mathbb{Q})). \tag{9}$$

It is well known that for a finite morphism $\phi\colon \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$, one has that $N(\phi(\mathbb{P}^1(\mathbb{Q})); h) \asymp h^{2/\deg \phi}$. Moreover, in the special case that ϕ is geometrically Galois, $N(\phi(\mathbb{P}^1(\mathbb{Q})); h) \sim \kappa(\phi) \cdot h^{2/\deg \phi}$ for some explicitly computable constant $\kappa(\phi) > 0$. We give a detailed proof of these results in Section 3 for completeness. Combining this with the partition Equation (9) implies that

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

where the sum is restricted to those $\rho\colon \mathrm{Gal}(L|\mathbb{Q}) \hookrightarrow G$ in $\mathrm{H}_{\mathcal{S}}(\mathbb{Q}, G)$ for which the twist Z_ρ is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$. In particular, the constant $\kappa((2,2,2), \mathcal{S})$ will be the sum of the constants $\kappa(\phi_\rho)$.

Step 3: (Sieving) The count above already contains the count of the proper subset $\Omega(F_3) \subset \Omega_{\mathcal{S}}(2,2,2)$ that we seek. Indeed, starting from the partition (9), we note that, since the twists ϕ_ρ are (Galois) Belyi maps of signature $(2,2,2)$, we can assign to each $\rho \in \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, G)$ a unique 2-simplified coefficient (A_ρ, B_ρ, C_ρ) such that $\phi_\rho(Z_\rho(\mathbb{Q}))$ is contained in the set $\Omega(F_\rho)$, associated to the generalized Fermat equation

$$F_\rho\colon A_\rho \mathsf{x}^2 + B_\rho \mathsf{y}^2 + C_\rho \mathsf{z}^2 = 0.$$

In particular, we deduce that some twist of $\phi_0\colon Z_0 \to \mathbb{P}^1$ is isomorphic to $\phi_3\colon Z_3 \to \mathbb{P}^1$, and that $\Omega(F_3) = \Omega(\phi_3(Z_3(\mathbb{Q}))$. In Example 3.5, we calculate that $\kappa(F_3) = 1/\pi$, and we conclude that

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

□

1.5. **Previous work on spherical Fermat equations.** This work is closely related to, and inspired by, the foundational contributions of Beukers [Beu98]. Indeed, the arguments in Section 4 can be slightly modified to reprove [Beu98, Theorem 1.2]. On a related note, the excellent Master's thesis of Esmonde [Esm99] addresses the problem of solving the equation $\mathsf{x}^a + \mathsf{y}^b - \mathsf{z}^c = 0$ in polynomial rings $k[t]$, for certain examples of fields k. Building on work of Beukers, Edwards [Edw04] completed the parametrizations of the spherical equations $\mathsf{x}^2 + \mathsf{y}^3 - \mathsf{z}^3 = 0$, $\mathsf{x}^2 + \mathsf{y}^3 - \mathsf{z}^4 = 0$, and $\mathsf{x}^2 + \mathsf{y}^3 - \mathsf{z}^5 = 0$. We expect that the method of Fermat descent employed here can be extended to compute parametrizations for general spherical Fermat equations; this is work in progress by the author.

Acknowledgments. This work is part of the author's PhD thesis. We thank David Zureick-Brown, John Voight, and Andrew Kobin for many enlightening conversations on this topic and for their valuable feedback. We are also grateful to Bjorn Poonen for agreeing to serve on the thesis committee and for his detailed and insightful comments on an earlier draft.

2. Belyi maps and triangle groups

2.1. **(Spherical) triangle groups.**

We follow [CV19, Section 2]. For more on this topic see [Mag74, 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 2.1. Given integers $a, b, c > 1$, 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

$$\delta_0^a = \delta_1^b = \delta_\infty^c = \delta_0\delta_1\delta_\infty = -1. \tag{10}$$

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

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 Klein more than a century ago. By [CV19, Remark 2.2], reordering the signature (a, b, c) to be nondecreasing $a \leqslant b \leqslant c$ does not affect the isomorphism class of $\bar{\triangle}(a, b, c)$.

- 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 $\bar{\Delta}(2,3,5)$ is isomorphic to A_5; the group of rigid motions of the icosahedron.

Table 2. 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	$1/30$

2.2. **(Spherical) Belyi maps.** By curve we mean a separated scheme of finite type over a field of dimension one. We say that a curve is nice if it is smooth, projective, and geometrically irreducible.

Definition 2.2. Let Z_k be a nice curve defined over a perfect field k. A k-Belyi map is a finite k-morphism $\phi\colon Z_k \to \mathbb{P}^1_k$ that is unramified outside $\{0,1,\infty\} \subset \mathbb{P}^1(k)$.

Remark 2.3. 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 [Bel79, Bel02]. For this reason, it is customary to require that $k \subset \mathbb{C}$ to use the term *Belyi* map. We ignore this convention, and allow k to be perfect of positive characteristic.

Definition 2.4. Let $\phi\colon Z_k \to \mathbb{P}^1_k$ be a k-Belyi map with automorphism k-group scheme $\mathrm{Aut}(\phi)$. We say that ϕ is geometrically Galois if the extension of function fields $\mathbf{k}(Z_{\bar{k}}) \supset \mathbf{k}(\mathbb{P}^1_{\bar{k}})$ is Galois, with Galois group denoted by $\mathrm{Gal}(\phi)$. Equivalently, ϕ is geometrically Galois if $\mathbf{Aut}(\phi)(\bar{k}) = \mathrm{Aut}(\phi_{\bar{k}})$ acts transitively on the fibers. This is the case if and only if $\mathrm{Aut}(\phi_{\bar{k}}) \cong \mathrm{Gal}(\phi)$.

Remark 2.5. 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 $\mathrm{Gal}(\phi)$-torsor over $\mathrm{Spec}\, k$.

Definition 2.6. The signature of a geometrically Galois k-Belyi map $\phi\colon Z_k \to \mathbb{P}^1_k$ is the triple (e_0, e_1, e_∞) where e_P is the ramification index $e_\phi(z)$ of any critical point $z \in Z_k$ with critical value $P \in \{0, 1, \infty\}$. The Euler characteristic of ϕ is the quantity

$$\chi(\phi) := \tfrac{1}{e_0} + \tfrac{1}{e_1} + \tfrac{1}{e_\infty} - 1. \tag{11}$$

As a consequence of the Riemann Existence Theorem, there exist Galois Belyi maps of any spherical signature. See [DG95, Proposition 3.1] and [Poo05, Lemma 2.5] for a proof of the following proposition.

Proposition 2.7. *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 Galois group of ϕ. Then $2 - 2g = (\deg\phi)\cdot\chi(\phi)$. In particular,*

(i) If $\chi(\phi) > 0$, then $g = 0$ and $\deg\phi = \#G = 2/\chi(\phi)$.
(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 geometrically Galois Belyi defined over $\mathbb{Q}$. The reader may find several examples in the Belyi maps LMFDB beta database [LMF25]. The maps presented in Table 2 are adapted from the parametrizations found in [Coh07, Chapter 14]. The original sources are [Beu98] and [Edw04].

TABLE 3. Examples of geometrically Galois $\mathbb{Q}$-Belyi maps for the spherical signatures.

(a,b,c)	$\bar{\triangle}(a,b,c)$	Example
$(2,2,c)$	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. Counting rational points the image of a rational function

The results presented in this section are undoubtedly well known ([Ser97, p. 133], [HS00, Theorem B.6.1]); however, authors often ignore the leading constants we seek. For completeness, we provide full proofs, making the leading constants explicit.

Situation 3.1. 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 nonconstant $\mathbb{Q}$-morphism with $d := \deg(\phi)$.
- 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 3.2. *We have $N(\Omega(\phi); h) \asymp h^{2/d}$ as $h \to \infty$. More precisely, there exists an explicitly computable constant $\delta(\phi) > 0$ such that*
$$\tfrac{1}{d} \cdot \delta(\phi) \cdot h^{2/d} \leqslant N(\Omega(\phi)); h) \leqslant \delta(\phi) \cdot h^{2/d}, \qquad \textit{as } h \to \infty.$$
The constant $\delta(\phi)$ is described in Equation (19).

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 3.2 to an asymptotic count.

Corollary 3.3. *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
$$\kappa(\phi) = \delta(\phi) / \#\,\mathrm{Aut}(\phi),$$
and the implied constant depends on ϕ and ε.

3.1. **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

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

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

$$\begin{tikzcd}
\mathbb{P}^1(\mathbb{Q}) \arrow[dd, "\phi"'] & \mathcal{V}(\mathbb{Z}) \arrow[l] \arrow[dr, "\tilde{\phi}"] & \\
 & & \mathbb{Z}^2 \arrow[dl, "\cdot(1/\gcd)"] \\
\mathbb{P}^1(\mathbb{Q}) & \mathcal{V}(\mathbb{Z}) \arrow[l] &
\end{tikzcd}$$

Define the primitivity defect set of ϕ by

$$\mathcal{D}(\phi) := \left\{ \gcd \tilde{\phi}(s,t) : (s,t) \in \mathcal{V}(\mathbb{Z}) \right\}. \tag{12}$$

The set $\mathcal{D}(\phi)$ is finite. Indeed, let $R(\phi) \in \mathbb{Z}$ denote the resultant of the homogeneous polynomials ϕ_0 and ϕ_∞. Then, every primitivity defect divides $R(\phi)$.

Lemma 3.4. *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

$$\mathcal{V}(\mathbb{Z}) = \bigsqcup_{e \in \mathcal{D}(\phi)} \mathcal{V}(\mathbb{Z})_e. \tag{13}$$

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

$$\mathbb{Z} \cdot \mathcal{V}(\mathbb{Z})_e := \{(ns, nt) : n \in \mathbb{Z}, (s,t) \in \mathcal{V}(\mathbb{Z})_e\} \subset \mathbb{Z}^2.$$

From the partition Figure 1 of primitive points, we obtain the partition

$$\mathbb{Z}^2 = \bigsqcup_{e \in \mathcal{D}(\phi)} \mathbb{Z} \cdot \mathcal{V}(\mathbb{Z})_e. \tag{14}$$

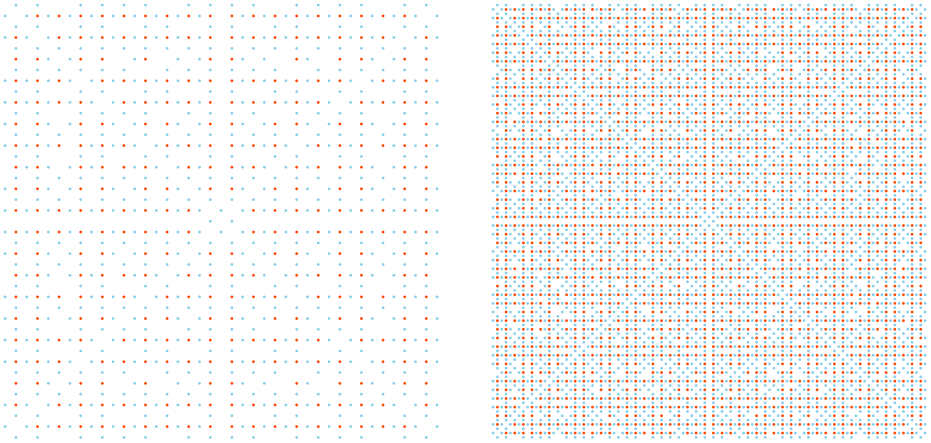

FIGURE 1. Partition $\mathcal{V}(\mathbb{Z}) = \mathcal{V}(\mathbb{Z})_1 \sqcup \mathcal{V}(\mathbb{Z})_4$ with respect to the Galois map $\phi(s:t) = ((s^2-t^2)^2 : (s^2+t^2)^2)$, with primitivity defect set $\mathcal{D}(\phi) = \{1, 4\}$.

3.2. **Proof of Proposition 3.2 and Corollary 3.3.** We start with the proof of the asymptotic bounds. We will abbreviate

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

Proof of Proposition 3.2. We may apply the principle of Lipschitz [Dav51] to obtain

$$\begin{aligned} \widetilde{M}(h) &:= \# \left\{ (s,t) \in \mathbb{Z}^2 : \max \tilde{\phi}(s,t) \leqslant h \right\} \\ &= \operatorname{vol}(\mathcal{R}_1) \cdot h^{2/d} + O\left(h^{1/d}\right), \end{aligned} \tag{15}$$

where $\operatorname{vol}(\mathcal{R}_1)$ is the Lebesgue measure of the compact region $\mathcal{R}_1$ in $\mathbb{R}^2$ given by $\max\{|\phi_0(s,t)|, |\phi_\infty(s,t)|\} \leqslant 1$.

In light of the partition Equation (14), we see that for each $e \in \mathcal{D}(\phi)$ the set $\mathbb{Z} \cdot \mathcal{V}(\mathbb{Z})_e$ has a density $\delta_e \in [0,1]$, and $\sum_{e \in \mathcal{D}(\phi)} \delta_e = 1$. Moreover, if we define

$$\widetilde{M}_e(h) := \# \left\{ (s,t) \in \mathbb{Z} \cdot \mathcal{V}(\mathbb{Z})_e : \max \tilde{\phi}(s,t) \leqslant h \right\},$$

then $\widetilde{M}_e(h) = \delta_e \cdot \widetilde{M}(h) + O(1)$.

We apply a standard Möbius sieve to Equation (15) to obtain, for every $\varepsilon > 0$, the asymptotic

$$\begin{aligned}\widetilde{N}(h) &:= \#\left\{(s,t) \in \mathcal{V}(\mathbb{Z}) : \max \tilde{\phi}(s,t) \leqslant h\right\}\\ &= \frac{6}{\pi^2} \cdot \operatorname{vol}(\mathcal{R}_1) \cdot h^{2/d} + O_{e,\varepsilon}\left(h^{1/d+\varepsilon}\right). \qquad (16)\end{aligned}$$

Moreover, if we define

$$\widetilde{N}_e(h) := \#\left\{(s,t) \in \mathcal{V}(\mathbb{Z})_e : \max \tilde{\phi}(s,t) \leqslant h\right\},$$

then $\widetilde{N}_e(h) = \delta_e \cdot \widetilde{N}(h) + O(1)$. Consider the counting function

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

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

$$\tfrac{1}{d} \cdot N(h) \leqslant N(\Omega(\phi); h) \leqslant N(h), \qquad (17)$$

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 $N(h)$ to the counting functions $\widetilde{N}_e(h)$. By the definition of Ht, we see that

$$\begin{aligned}N(h) &= \frac{1}{2} \sum_{e \in \mathcal{D}(\phi)} \widetilde{N}_e(eh)\\ &= \frac{1}{2} \sum_{e \in \mathcal{D}(\phi)} \left(\frac{6}{\pi^2} \cdot \operatorname{vol}(\mathcal{R}_1) \cdot \delta_e \cdot (eh)^{2/d} + O\left((eh)^{1/d+\varepsilon}\right)\right)\\ &= \frac{3}{\pi^2} \operatorname{vol}(\mathcal{R}_1) \left(\sum_{e \in \mathcal{D}(\phi)} \delta_e \cdot e^{2/d}\right) \cdot h^{2/d} + O\left(h^{1/d+\varepsilon}\right). \qquad (18)\end{aligned}$$

In particular, the leading constant is

$$\delta(\phi) = \frac{3}{\pi^2} \operatorname{vol}(\mathcal{R}_1) \left(\sum_{e \in \mathcal{D}(\phi)} \delta_e \cdot e^{2/d}\right). \qquad (19)$$

□

We will use Proposition 3.2 in the special case of a geometrically Galois $\mathbb{Q}$-Belyi map ϕ.

Proof of Corollary 3.3. Suppose that ϕ is geometrically Galois, with Galois group $\operatorname{Gal}(\phi) = \operatorname{Aut}(\phi_{\overline{\mathbb{Q}}})$. Then, $\operatorname{Gal}(\phi)$ 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

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

Indeed $\operatorname{Aut}(\phi) = \operatorname{Aut}(\phi_{\bar{\mathbb{Q}}})^{\operatorname{Gal}_{\mathbb{Q}}}$, and for every $P \in \phi^{-1}(Q)(\mathbb{Q})$ and $\gamma \in \operatorname{Aut}(\phi)$, 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 $\gamma \in \operatorname{Aut}(\phi_{\bar{\mathbb{Q}}})$ such that $\gamma(P') = P$. For any $\sigma \in \operatorname{Gal}_{\mathbb{Q}}$, 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 $\gamma \in \operatorname{Aut}(\phi)$. It follows that $N_\phi(h) = \#\operatorname{Aut}(\phi) \cdot N(\Omega(\phi); h)$, and the proof is complete. In particular, the leading constant is

$$\kappa(\phi) = \frac{3}{\pi^2}\frac{\operatorname{vol}(\mathcal{R}_1)}{\#\operatorname{Aut}(\phi)}\left(\sum_{e\in\mathcal{D}(\phi)} \delta_e \cdot e^{2/d}\right). \tag{20}$$

□

Example 3.5 (Pythagorean constant)**.** In Section 1.4, we concluded that for $F\colon \mathsf{x}^2 + \mathsf{y}^2 - \mathsf{z}^2 = 0$, we have the identity $\Omega(F) = \Omega(\phi)$, where $\phi\colon Z := \operatorname{Proj}\mathbb{Q}[\mathsf{x},\mathsf{y},\mathsf{z}]/(\mathsf{x}^2+\mathsf{y}^2-\mathsf{z}^2) \to \mathbb{P}^1_{\mathbb{Q}}$ is the Galois Belyi map $(x : y : z) \mapsto (x^2 : z^2)$. Take the isomorphism $\mathbb{P}^1 \cong Z$ given by $(s : t) \mapsto (s^2 - t^2 : 2st : s^2 + t^2)$, and rename ϕ to be the composition $\mathbb{P}^1 \cong Z \to \mathbb{P}^1$, $(s : t) \mapsto ((s^2-t^2)^2 : (s^2+t^2)^2)$.

- Since $\max\{|s^2 - t^2|^2, |s^2 + t^2|^2\} = (s^2 + t^2)^2$, the region $\mathcal{R}_1$ is the unit disc, and $\operatorname{vol}(\mathcal{R}_1) = \pi$.
- The primitivity defect set $\mathcal{D}(\phi) = \{1, 4\}$. The densities are $\delta_1 = 2/3$ and $\delta_4 = 1/3$.

Putting this data into Equation (19), we see that

$$\delta(\phi) = \frac{3}{\pi^2} \cdot \pi \left(\frac{2}{3} + \frac{4^{2/4}}{3}\right) = \frac{4}{\pi}.$$

Finally, since $\operatorname{Aut}(\phi) \cong G \cong C_2 \times C_2$, we obtain $\kappa(\phi) = \delta(\phi)/4 = \frac{1}{\pi}$.

4. Proof of main results

Situation 4.1. We adopt the following notation for the rest of this section.

- Let (a, b, c) be a spherical signature (see Table 2), we do not assume that $a \leqslant b \leqslant c$.
- Let $\mathcal{S}$ denote a finite set of primes, and $R = \mathbb{Z}[\mathcal{S}^{-1}]$.
- Recall that $\mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, G)$ denotes the Galois cohomology pointed set which classifies G-torsors over $\operatorname{Spec}\mathbb{Q}$ unramified outside of $\mathcal{S}$.

- For any $\Omega \subset \mathbb{P}^1(\mathbb{Q})$, and any $h > 0$, we have the counting function $N(\Omega; h)$ defined in Situation 3.1.

Our proof follows the guidelines of the method of Fermat descent, as presented in [AP25]. It consists on three steps: covering, twisting, and sieving.

4.1. **Covering.** The covering is a geometrically Galois $\mathbb{Q}$-Belyi map $\phi\colon \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ with signature (a, b, c). For instance we can always start with one of the maps described by the rational functions in Table 3 and, since we are not assuming that $a \leqslant b \leqslant c$, compose with an appropriate permutation $\gamma \in \mathrm{PGL}_2(\mathbb{Q})$ of $\{0, 1, \infty\}$.

4.2. **Twisting.** By [AP25, Lemma 3.23], there exists a finite set of primes $\mathcal{S}$ for which the map ϕ admits an R-model $\Phi\colon \mathbb{P}^1_R \to \mathbb{P}^1_R$ such that $\mathbb{P}^1(a, b, c)_R \cong [\mathbb{P}^1_R / \mathbf{Aut}(\Phi)]$. Descent theory gives the partition

$$\begin{aligned}\mathbb{P}^1(a, b, c)\langle R\rangle &= \bigsqcup_{\tau \in \mathrm{H}^1(R, \mathbf{Aut}(\Phi))} \Phi_\tau(\mathbb{P}^1_\tau(R)) \\ &= \bigsqcup_{\tau \in \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, \mathrm{Gal}(\phi))} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})).\end{aligned}$$

Here, $\mathrm{H}^1(R, \mathbf{Aut}(\Phi))$ denotes the fppf Čech cohomology pointed set. It is in bijection with isomorphism classes of fppf $\mathbf{Aut}(\Phi)$-torsor schemes $T \to \operatorname{Spec} R$. Restriction to the generic fiber induces an isomorphism

$$\mathrm{H}^1(R, \mathbf{Aut}(\Phi)) \cong \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, \mathrm{Gal}(\phi))$$

of pointed sets. Note that $\mathrm{Gal}(\phi) \cong \mathbf{Aut}(\phi)(\bar{\mathbb{Q}}) = \mathrm{Aut}(\phi_{\bar{\mathbb{Q}}})$, so the action of the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}}$ is the natural one. In general, $\mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, \mathrm{Gal}(\phi))$ is only a pointed set and not a group, since $\mathrm{Gal}(\phi) \cong \bar{\Delta}(a, b, c)$ as abstract groups, and the only abelian spherical triangle group is $\bar{\Delta}(2, 2, 2) \cong C_2 \times C_2$. Crucially, the set $\mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, \mathrm{Gal}(\phi))$ is finite, and classifies twists of the Belyi map ϕ. It is worth noting that in some cases, the source curve of a twist $\phi_\tau\colon \mathbb{P}^1_\tau \to \mathbb{P}^1$ might be a pointless conic. Nevertheless, since the equations

$$\begin{aligned}\mathsf{x}^2 + \mathsf{y}^2 - \mathsf{z}^c &= 0, \quad (c \geqslant 2) \\ \mathsf{x}^2 + \mathsf{y}^3 - \mathsf{z}^3 &= 0, \\ \mathsf{x}^2 + \mathsf{y}^3 - \mathsf{z}^4 &= 0, \\ \mathsf{x}^2 + \mathsf{y}^3 - \mathsf{z}^5 &= 0,\end{aligned}$$

all have primitive integral solutions, we know that $\Omega(a, b, c) \neq \varnothing$, and there will always be at least one twist for which $\mathbb{P}^1_\tau(\mathbb{Q}) \neq \varnothing$.

4.3. **Sieving.** Combining the partition above with Corollary 3.3, we obtain

$$N(\Omega_{\mathcal{S}}(a,b,c);h) = \sum_{\tau} N(\Omega(\phi_\tau);h),$$

where the sum ranges over all the $\tau \in \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, \mathrm{Gal}(\phi))$ for which $\mathbb{P}^1_\tau$ is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$. To sieve out the excess of elements in $\mathbb{P}^1(a,b,c)\langle R\rangle$ not corresponding to points in $\Omega(a,b,c) = \mathbb{P}^1(a,b,c)\langle\mathbb{Z}\rangle$, we show that we can restrict to certain subsets $T(F) \subset T(a,b,c) \subset \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, \mathrm{Gal}(\phi))$ to cover all of $\Omega(F)$ and $\Omega(a,b,c)$. The proofs of both Theorem 1.2 and Theorem 1.3 (in the special case of simplified equations (Definition 1.5)) will follow immediately from the following lemma.

Lemma 4.2. *Fix a possibly empty subset $\mathcal{T} \subset \mathcal{S}$. Take a $\mathcal{T}$-simplified Fermat equation $F\colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0$. Then, there is a finite subset $T(F) \subseteq \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, \mathrm{Gal}(\phi))$ such that*

$$\Omega(F) = \bigsqcup_{\tau \in T(F)} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})). \tag{21}$$

Moreover, defining $T(a,b,c)$ as the disjoint union of the sets $T(F)$, as F ranges over all $\varnothing$-simplified Fermat equations of signature (a,b,c), we have

$$\Omega(a,b,c) = \bigsqcup_{\tau \in T(a,b,c)} \phi_\tau(\mathbb{P}^1_\tau(\mathbb{Q})). \tag{22}$$

Proof. Any geometrically Galois $\mathbb{Q}$-Belyi map $\phi\colon \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ of signature (a,b,c) is given by a rational function

$$\frac{\phi_0}{\phi_\infty} = 1 + \frac{\phi_1}{\phi_\infty} \in \mathbf{k}(\mathbb{P}^1_{\mathbb{Q}}),$$

where

(i) $\phi_0, \phi_1, \phi_\infty \in \mathbb{Z}[\mathsf{s},\mathsf{t}]$ are homogeneous of degree $\#\bar{\Delta}(a,b,c)$,
(ii) $\gcd(\phi_0,\phi_\infty) = \gcd(\phi_1,\phi_\infty) = 1$, and
(iii) we can write

$$\phi_0(\mathsf{s},\mathsf{t}) = C_0 \cdot X(\mathsf{s},\mathsf{t})^a,$$
$$\phi_1(\mathsf{s},\mathsf{t}) = C_1 \cdot Y(\mathsf{s},\mathsf{t})^b,$$
$$\phi_\infty(\mathsf{s},\mathsf{t}) = C_\infty \cdot Z(\mathsf{s},\mathsf{t})^c,$$

for unique polynomials $X, Y, Z \in \mathbb{Z}[\mathsf{s},\mathsf{t}]$, and a unique triple (C_0, C_1, C_∞) of $\mathcal{S}(\phi)$-simplified Fermat coefficients, where $\mathcal{S}(\phi)$ is an explicit set of bad primes.

We denote this triple by $\mathbf{sfc}(\phi)$. Observe that for any $Q \in \mathbb{P}^1(\mathbb{Q})$, we have that $\mathbf{sfc}(\phi) = \mathbf{sfc}(\phi(Q))$.

Returning to the situation of this section, to each cohomology class τ we can associate the $\mathcal{S}$-simplified Fermat coefficient triple $\mathbf{sfc}(\phi_\tau)$. If F is $\mathcal{T}$-simplified, then it is also $\mathcal{S}$-simplified. Moreover, for every primitive integral solution (x, y, z) to F, the point $j(x, y, z) \in \mathbb{P}^1(\mathbb{Q})$ is in $\Omega_{\mathcal{S}}(a, b, c)$. Define

$$T(F) := \left\{\tau \in \mathrm{H}^1_{\mathcal{S}}(\mathbb{Q}, \mathrm{Gal}(\phi)) : \mathbf{sfc}(\phi_\tau) = (A, B, C)\right\}.$$

□

To finish the proof of Theorem 1.3, we must consider the case of non-simple equations. To guide our intuition, consider the equation $F' \colon 25\mathsf{x}^2 + \mathsf{y}^2 = \mathsf{z}^2$. Our strategy is to use the *simplification* $F \colon \mathsf{x}^2 + \mathsf{y}^2 = \mathsf{z}^2$ to deduce the asymptotic result for F' from that of F. In this case, the $\mathbb{Q}$-isomorphism of nice curves $C \to C'$, $\quad (x : y : z) \mapsto (x/5 : y : z)$ enables this translation. The idea is that the congruence condition $x \equiv 0 \bmod 5$ cuts out a positive proportion of the primitive integral solutions to the Pythagorean equation, and only the constant term in the asymptotic will change.

Start with a non-simple equation $F' \colon A'\mathsf{x}^a + B'\mathsf{y}^b + C'\mathsf{z}^c = 0$. Without loss of generality, we may assume that $\gcd(A', B', C') = 1$. In this case, we can write

$$A' = A \cdot A_0^a, \quad B' = B \cdot B_1^b, \quad C' = C \cdot C_\infty^c,$$

to obtain a $\mathcal{T}$-simplified coefficient triple (A, B, C), where $\mathcal{T}$ is the set of primes dividing $A' \cdot B' \cdot C'$. The Fermat equation $F \colon A\mathsf{x}^a + B\mathsf{y}^b + C\mathsf{z}^c = 0$ is the simplification of F'. From Lemma 4.2, we have a partition

$$\Omega(F) = \bigsqcup_{\tau \in T(F)} \Omega(\phi_\tau), \tag{23}$$

where each ϕ_τ is a geometrically Galois $\mathbb{Q}$-Belyi maps $\mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ of signature (a, b, c). Let ϕ be one of these maps. We have seen that ϕ corresponds to a rational function

$$\phi = \frac{A \cdot X(\mathsf{s}, \mathsf{t})^a}{C \cdot Z(\mathsf{s}, \mathsf{t})^c} = 1 + \frac{B \cdot Y(\mathsf{s}, \mathsf{t})^b}{C \cdot Z(\mathsf{s}, \mathsf{t})^c}.$$

To conclude, we use a clever argument of Beukers [Beu98, Proof of Theorem 1.5]. Consider the polynomial map

$$\alpha \colon \mathbb{Q}^2 \to \mathbb{Q}^3, \quad (s, t) \mapsto \left(\frac{X(s, t)}{A_0}, \frac{Y(s, t)}{B_1}, \frac{Z(s, t)}{C_\infty}\right). \tag{24}$$

We use α to define a lattice of rank two generated by the points whose image is integral

$$\Lambda(\alpha) := \mathrm{Span}_{\mathbb{Z}} \left\{(s,t) \in \mathbb{Q}^2 : \alpha(s,t) \in \mathbb{Z}^3\right\}.$$

Choose an integral basis $\{\vec{\alpha}_1, \vec{\alpha}_2\}$ for $\Lambda(\alpha)$, and define

$$\phi' = \frac{A \cdot X(\mathsf{s}\vec{\alpha}_1 + \mathsf{t}\vec{\alpha}_2)^a}{C \cdot Z(\mathsf{s}\vec{\alpha}_1 + \mathsf{t}\vec{\alpha}_2)^c} = 1 + \frac{B \cdot Y(\mathsf{s}\vec{\alpha}_1 + \mathsf{t}\vec{\alpha}_2)^b}{C \cdot Z(\mathsf{s}\vec{\alpha}_1 + \mathsf{t}\vec{\alpha}_2)^c}.$$

Applying this construction to every ϕ_τ appearing in Equation (23), we obtain the partition

$$\Omega(F') = \bigsqcup_{\tau \in T(F)} \Omega(\phi'_\tau),$$

from which we conclude the proof.

References

[AP25] Santiago Arango-Piñeros, *Fermat descent*, arXiv e-prints (2025), arXiv:2508.13059.

[Bel79] G. V. Belyi, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276, 479. MR 534593

[Bel02] ______, *A new proof of the three-point theorem*, Mat. Sb. **193** (2002), no. 3, 21–24. MR 1913596

[Beu98] Frits Beukers, *The Diophantine equation $Ax^p + By^q = Cz^r$*, Duke Math. J. **91** (1998), no. 1, 61–88. MR 1487980

[Coh07] Henri Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007. MR 2312338

[CV19] Pete L. Clark and John Voight, *Algebraic curves uniformized by congruence subgroups of triangle groups*, Trans. Amer. Math. Soc. **371** (2019), no. 1, 33–82. MR 3885137

[Dar97] H. Darmon, *Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation*, C. R. Math. Rep. Acad. Sci. Canada **19** (1997), no. 1, 3–14. MR 1479291

[Dav51] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183. MR 43821

[DG95] 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** (1995), no. 6, 513–543. MR 1348707

[Edw04] Johnny Edwards, *A complete solution to $X^2 + Y^3 + Z^5 = 0$*, J. Reine Angew. Math. **571** (2004), 213–236. MR 2070150

[Esm99] Indigo Esmonde, *Parametric solutions to the generalized fermat equation*, M.Sc. thesis, McGill University, 1999, Unpublished Master's thesis.

[HS00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction. MR 1745599

[Leh00] Derrick Norman Lehmer, *Asymptotic Evaluation of Certain Totient Sums*, Amer. J. Math. **22** (1900), no. 4, 293–335. MR 1505840

[LM55] J. Lambek and L. Moser, *On the distribution of Pythagorean triangles*, Pacific J. Math. **5** (1955), 73–83. MR 67911

[LMF25] The LMFDB Collaboration, *The L-functions and modular forms database (beta)*, https://beta.lmfdb.org/Belyi, 2025, [Online; accessed 24 July 2025].

[Mag74] Wilhelm Magnus, *Noneuclidean tesselations and their groups*, Pure and Applied Mathematics, vol. Vol. 61, Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1974. MR 352287

[Poo05] Bjorn Poonen, *Unramified covers of Galois covers of low genus curves*, Math. Res. Lett. **12** (2005), no. 4, 475–481. MR 2155225

[Poo06] ———, *The projective line minus three fractional points*, Slides for the MSRI program: Rational and integral points on higher-dimensional varieties, July 2006.

[PSS07] 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** (2007), no. 1, 103–158. MR 2309145

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, With a foreword by Brown and Serre. MR 1757192

Department of Mathematics, University of Massachusetts Amherst, Amherst, MA 01003, USA

Email address: santiago.arango.pineros@gmail.com

URL: https://sarangop1728.github.io/