Examples of Descent

Mark Saengrungkongka

March 4, 2026

Abstract

The main theorem of descent states that if X is a smooth proper variety over global field k, G is a smooth affine algebraic group over k, and $f : Z \to X$ is a G-torsor over X, then the k-rational points of X correspond to a union of k-rational points of finitely many twists of Z. This reduces the problem of finding rational points of X to finding rational points of finitely many twists of Z. We illustrate this theorem through several examples, including the Weak Mordell-Weil Theorem.

This article accompanies the talk given at the STAGE Seminar on March 5, 2026. The main reference is Sections 8.3-8.4 of [Poo17].

Throughout this article, a curve is **nice** if it is smooth, projective, and geometrically integral.

§1 Example: Rational Points on a Genus 2 Curve

We begin motivating descent by considering the following problem.

Example 1.1.

Find all $(x, y) \in \mathbb{Q}^2$ that satisfies an equation

$$y^2 = (x^2 + 1)(x^4 + 1). \tag{1}$$

§1.1 An Elementary Argument

Write $x = \frac{X}{Z}$ with $\gcd(X, Z) = 1$. Then we have

$$y^2 = \frac{(X^2 + Z^2)(X^4 + Z^4)}{Z^6}.$$

From $\gcd(X, Z) = 1$, we get that $\gcd((X^2 + Z^2)(X^4 + Z^4), Z^6) = 1$, so $y = \frac{Y}{Z^3}$ for some integer Y with $\gcd(Y, Z) = 1$. Thus, the problem is equivalent to finding $(X, Y, Z) \in \mathbb{Z}^3$ such that $\gcd(X, Z) = 1$ and

$$Y^2 = (X^2 + Z^2)(X^4 + Z^4).$$

To do this, we consider $\gcd(X^2 + Z^2, X^4 + Z^4)$. Note that

$$\begin{aligned}\gcd(X^2 + Z^2, X^4 + Z^4) &= \gcd(X^2 + Z^2, (X^4 + Z^4) - (X^2 + Z^2)^2) \\ &= \gcd(X^2 + Z^2, 2X^2Z^2).\end{aligned}$$

Since $\gcd(X^2 + Z^2, X^2Z^2) = 1$, it follows that $\gcd(X^2 + Z^2, X^4 + Z^4) \in \{1, 2\}$. However, the product $(X^2 + Z^2)(X^4 + Z^4)$ is a perfect square, so we deduce that

$$X^2 + Z^2 = cA^2, \quad X^4 + Z^4 = cB^2$$

for some integers A, B and $c \in \{1, 2\}$.

The integer solutions to $X^4 + Z^4 = cB^2$ corresponds to rational point on the genus 1 curve

$$Z_c : cy^2 = x^4 + 1.$$

When $c \in \{1, 2\}$, these curves are elliptic curves because there is one rational point, namely $(x, y) = (0, 1)$ for $c = 1$ and $(x, y) = (1, 1)$ for $c = 2$. Using these rational points, we can show that the curve Z_1 and Z_2 are birational to the curves

$$\begin{aligned} &\texttt{32.a3} \quad y^2 = x^3 - x \quad \text{and} \\ &\texttt{64.a3} \quad y^2 = x^3 - 4x, \end{aligned}$$

in the LMFDB, respectively. Both of these curves have Mordell-Weil rank 0, and the torsion groups are both isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. Using these rational points, we find that (1) has 6 solutions:

$$(0, \pm 1), (1, \pm 2), \text{ and } (-1, \pm 2).$$

§1.2 An Explanation

We are tasked to find rational points on the affine curve

$$\operatorname{Spec} \frac{\mathbb{Q}[x, y]}{(y^2 - (x^2 + 1)(x^4 + 1))},$$

which is birational to a nice curve of genus 2

$$X = \operatorname{Proj} \frac{\mathbb{Q}[x, y, z]}{(y^2 - (x^2 + z^2)(x^4 + z^4))},$$

where $\deg x = \deg z = 1$ and $\deg y = 3$. Note that the function field of X is

$$\mathbf{k}(X) = \mathbb{Q}\left(x, \sqrt{(x^2 + 1)(x^4 + 1)}\right).$$

In doing this, we use some elementary number-theoretic argument to reduce the problem of finding rational points of this genus 2 curve to finding rational points of two smaller genus 1 curves. To formalize this process, we let Z_c be the nice curve corresponding to the following system

$$\begin{aligned} y^2 &= (x^2 + 1)(x^4 + 1) \\ cw^2 &= x^4 + 1. \end{aligned}$$

Note that Z_c are twists of $Z_1 =: Z$. Observe that the function field of Z_c is

$$\mathbf{k}(Z_c) = \mathbb{Q}\left(x, \sqrt{c(x^2 + 1)}, \sqrt{c(x^4 + 1)}\right).$$

The obvious inclusion $\mathbf{k}(X) \hookrightarrow \mathbf{k}(Z_c)$ correspond to the degree 2 map

$$\begin{aligned} f_c : Z_c &\to X \\ (x, y, w) &\mapsto (x, y). \end{aligned} \tag{2}$$

Then the elementary argument above corresponds to two general facts that given $f : Z \to X$ with certain properties, then

(a) each rational point of X lies in the image of the twists f_c for some c;

(b) up to a multiplication by $\mathbb{Q}^{\times 2}$, there are finitely many c such that the twist Z_c of Z has a $\mathbb{Q}_p$-point for all primes p (including ∞). Moreover, this finite set is effectively computable.

(a) is a special case of Theorem 2.1, while (b) is a special case of Theorem 2.2.

§1.3 Galois Cover

Facts (a) and (b) above holds more generally when $f : Z \to X$ is a Galois cover. We recall the definition.

Definition 1.2.

An étale morphism of k-schemes $f : Z \to X$ is a **Galois cover** if there exists a finite group G of automorphisms of Z (as an X-scheme) such that the map

$$Z \times_k G \to Z \times_X Z,$$

given by (id, σ) from the piece corresponding to $\sigma \in G$, is an isomorphism. Here we view $G = \coprod_{g \in G} \operatorname{Spec} k$ as a discrete group.

If $f : Z \to X$ is a Galois cover, then we can do a descent argument to show that any rational point of X must be an image of a twisted map $f^\tau : Z^\tau \to X$ for a finite set of twists τ of f.

In the case where X and Z are curves, there is an even easier way to check that f is a Galois covering.

Proposition 1.3.

If $f : Z \to X$ is an étale morphism of nice curves such that the corresponding extension of function fields $\mathbf{k}(Z)/\mathbf{k}(X)$ is Galois, then f is a Galois cover.

▶ *Proof.* By the equivalence of categories of nice curves and function fields, any automorphism $\sigma \in \mathrm{Gal}(\mathbf{k}(Z)/\mathbf{k}(X))$ of $\mathbf{k}(Z)$ induces a right action on Z. This gives the desired subgroup of automorphisms. Above the generic point, the map $Z \times_k G \to Z \times_X Z$ is equal to the map

$$\mathbf{k}(Z) \otimes_{\mathbf{k}(X)} \mathbf{k}(Z) \to \mathbf{k}(Z) \times \mathbf{k}(Z) \times \cdots \times \mathbf{k}(Z)$$

sending $a \otimes b$ to $(a\sigma_1(b), \ldots, a\sigma_n(b))$ where $\mathrm{Gal}(\mathbf{k}(Z)/\mathbf{k}(X)) = \{\sigma_1, \ldots, \sigma_n\}$. Meanwhile, since the extension $\mathbf{k}(Z)/\mathbf{k}(X)$ is Galois, we have that $\mathbf{k}(Z) = \mathbf{k}(X)(\alpha)$ for some α that has minimal polynomial f of degree n. Then we have

$$\begin{aligned}
\mathbf{k}(Z) \otimes_{\mathbf{k}(X)} \mathbf{k}(Z) &\simeq \mathbf{k}(Z) \otimes_{\mathbf{k}(X)} \frac{\mathbf{k}(X)[t]}{(f(t))} \\
&\simeq \frac{\mathbf{k}(Z)[t]}{(f(t))} \\
&\simeq \frac{\mathbf{k}(Z)[t]}{(t - \sigma_1(\alpha))} \times \cdots \times \frac{\mathbf{k}(Z)[t]}{(t - \sigma_n(\alpha))} \\
&\simeq \mathbf{k}(Z) \times \cdots \times \mathbf{k}(Z).
\end{aligned}$$

Tracing the isomorphism through the above map gives the exact same map as above. Thus, the map $Z \times_k G \to Z \times_X Z$ is an isomorphism above the generic point. By spreading out, it is an isomorphism above a dense open neighborhood. Finally, both $Z \times_k Z$ and $Z \times_X Z$ are smooth, projective curve of dimension 1, so by valuative criterion of properness, the map is an isomorphism for the entire scheme. □

In our example, $f : Z \to X$ as defined in (2) is étale. Moreover, it has degree 2, so the extension of function fields is clearly Galois. Thus, $f : Z \to X$ is a Galois cover with Galois group $\mathbb{Z}/2$.

§2 Descent Obstruction via Torsors

In our example in Section 1, Z is a $\mathbb{Z}/2$-torsor over X. We now generalize state a general theorem that works for arbitrary torsors.

We let

- k be a global field;
- X be a k-variety;
- G be a smooth affine algebraic group over field k;
- Z be a G-torsor over X, together with a map $f : Z \to X$; and
- ζ be a class of Z in $\check{\mathrm{H}}^1_{\mathrm{fppf}}(X, G)$

Any point $x \in X(k)$ turns the map $f : Z \to X$ into the map of fibers $Z_x \to \operatorname{Spec} k$, making Z_x a G-torsor over k. The class corresponding to Z_x is denoted $\zeta(x) \in \mathrm{H}^1(k, G)$.

For any $\tau \in \mathrm{H}^1(k, G)$, we let $f^\tau : Z^\tau \to X$ be the twisted torsor.

The following theorem is a generalization of fact (a) introduced in Section 1.

Theorem 2.1.

For any $x \in X(k)$, we have

$$\zeta(x) = \tau \text{ if and only if } x \in f^\tau(Z^\tau(k)).$$

In particular, any rational point of $X(k)$ must be in $f^\tau(Z^\tau(k))$ for some $\tau \in \mathrm{H}^1(k, G)$.

▶ *Proof.* Let T be the G-torsor over k corresponding to τ. Each of the following is equivalent to the next.

- $x \in f^\tau(Z^\tau(k))$.
- there exists a point $y \in Z^\tau(k)$ (in particular $f(y) = x$);
- the fiber Z^τ_x is a trivial G^τ-torsor over k (since a torsor is trivial if and only if it has a rational point).
- $Z_x \overset{G}{\times} T^{-1}$ is trivial G^τ-torsor.
- $Z_x \simeq T$ as G-torsor (by taking contracted product with T on the right).
- $\zeta(x) = \tau$. □

We now describe how the argument Section 1 works in this abstract setting. For each place v of k, the inclusion $k \to k_v$ induces the map $\mathrm{H}^1(k, G) \to \mathrm{H}^1(k_v, G)$. Let this map sends $\tau \in \mathrm{H}^1(k, G)$ to $\tau_v \in \mathrm{H}^1(k_v, G)$.

Analogous to above, any point $x_v \in X(k_v)$ correspond to the class $\zeta_v(x) \in \mathrm{H}^1(k_v, G)$, giving a map $X(k_v) \to \mathrm{H}^1(k_v, G)$, making the following diagram commutes

$$\begin{array}{ccc} X(k) & \longrightarrow & \mathrm{H}^1(k, G) \\ \downarrow & & \downarrow \\ X(k_v) & \longrightarrow & \mathrm{H}^1(k_v, G) \end{array} \tag{3}$$

We define the **Selmer set**

$$\mathrm{Sel}_Z(k, G) = \{\tau \in \mathrm{H}^1(k, G) : \tau_v \in \mathrm{Im}(X(k_v) \to \mathrm{H}^1(k_v, G)) \text{ for all } v\}.$$

In particular, from (3) and Theorem 2.1, we get that

$$X(k) = \coprod_{\tau \in \mathrm{Sel}_Z(k,G)} f^\tau(Z^\tau(k)).$$

Now, we have the following big theorem that generalizes fact (b).

Theorem 2.2.

If X is proper, then we have that $\mathrm{Sel}_Z(k, G)$ is finite (and effectively computable).

▶ *Proof.* See Poonen's book. □

§3 Weak Mordell-Weil Theorem

Let k be a global field. Let A be an abelian variety over k, i.e., a projective variety with commutative group law. (An example of variety are elliptic curves and Jacobians of curves.)

Theorem 3.1 (Mordell-Weil Theorem)**.**

The group $A(k)$ is finitely-generated.

The first step to prove this theorem is to prove the following weaker version.

Theorem 3.2 (Weak Mordell-Weil Theorem)**.**

If m an integer not divisible by $\mathrm{char}\, k$, then the group $A(k)/mA(k)$ is finite.

Once we have this weaker version, the full Mordell-Weil theorem can be proven using height functions. Over $\mathbb{Q}$, the height is the maximum of logarithm of numerator and denominator. By analyzing how height changes under multiplication-by-2 map, we can deduce the full Mordell-Weil theorem from this weak version. We refer the reader to [HS00, Thm. C.0.1] for more details.

▶ *Proof of Weak Mordell-Weil theorem.* Let $G = A[m] = A(\overline{k})[m]$ denote the m-torsion group of A (over $\overline{k}$). Since m is not divisible by $\mathrm{char}\, k$, the multiplication-by-m map $[m] : A \xrightarrow{\cdot m} A$ is étale (see Poonen, Proposition 5.7.4) and promotes A to an G-torsor over A. This induces an evaluation map

$$\begin{aligned} A(k) &\to \mathrm{H}^1(k, G) \\ x &\mapsto \text{the class of } [m]^{-1}x. \end{aligned}$$

The image of this group is contained the Selmer set $\mathrm{Sel}_A(k, G)$, which is finite by Theorem 2.2. We now show that the kernel of this map is $mA(k)$. On one hand, if $x \in mA(k)$, then let $x = my$ for some $y \in A(k)$, and the isorphism from $[m]^{-1}x$ to the trivial torsor $\mathbf{G}$ is just subtraction by y.

In the other direction, note that if x maps to $0 \in \mathrm{H}^1(k, G)$, then the fiber $[m]^{-1}x$ is isomorphic to G. Let point $y \in [m]^{-1}x$ correspond to $0 \in G$. Then $y \in A(k)$, which implies that $x = my \in mA(k)$, as desired.

Hence, the map above induces a map $A(k)/mA(k) \to \mathrm{Sel}_A(k, G)$, so $A(k)/mA(k)$ is finite. □

For concreteness, let us write down what's going on in the case of

- $k = \mathbb{Q}$;
- $m = 2$;
- $A = E$ is an elliptic curve such that $E[2] \subseteq E(\mathbb{Q})$

In this case, suppose that the elliptic curve E is of the form $y^2 = (x-a)(x-b)(x-c)$ for some $a, b, c \in \mathbb{Q}$.

Then we are doing descent on the muliplication-by-2 map $[2] : E \xrightarrow{\cdot 2} E$. Given point $P = (X, Y) \in \mathbb{Q}^2$ on this elliptic curve, the x-coordinates of the preimages $[2]^{-1}P$ are

$$\begin{aligned}
&X + \sqrt{(X-a)(X-b)} + \sqrt{(X-b)(X-c)} + \sqrt{(X-c)(X-a)},\\
&X - \sqrt{(X-a)(X-b)} - \sqrt{(X-b)(X-c)} + \sqrt{(X-c)(X-a)},\\
&X + \sqrt{(X-a)(X-b)} - \sqrt{(X-b)(X-c)} - \sqrt{(X-c)(X-a)},\\
&X - \sqrt{(X-a)(X-b)} + \sqrt{(X-b)(X-c)} - \sqrt{(X-c)(X-a)}.
\end{aligned}$$

What happen if we try to use an elementary argument again? Note that $\gcd$ of any two of $X-a$, $X-b$, and $X-c$, is bounded. In particular, for some fixed finite subset $T \subset (\mathbb{Q}/\mathbb{Q}^{\times 2})^3$, there exists $(\alpha, \beta, \gamma) \in T$ such that

$$X - a = \alpha U^2, \quad X - b = \beta V^2, \quad X - c = \gamma W^2$$

for some $U, V, W \in \mathbb{Q}$.

The upshot of this is that the points $[2]^{-1}P$ is in a number field $\mathbb{Q}(\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\gamma})$, which is small and has finitely many possible such fields.

This corresponds to the Selmer group calculation. In fact, we have that

$$\mathrm{Sel}_E(k, E[2]) \simeq \left\{ (\alpha, \beta, \gamma) \in (\mathbb{Q}/\mathbb{Q}^{\times 2})^3 : \begin{array}{c} X - a = \alpha U^2,\ X - b = \beta V^2,\ X - c = \gamma W^2 \\ \text{has a solution } (X, U, V, W) \in \mathbb{A}^4_{\mathbb{Q}} \end{array} \right\},$$

and the group structure is given by componentwise multiplication in $(\mathbb{Q}/\mathbb{Q}^{\times 2})^3$. (The fact that if P is sent to (α, β, γ) and Q is sent to $(\alpha', \beta', \gamma')$, then $P + Q$ is sent to $(\alpha\alpha', \beta\beta', \gamma\gamma')$ can also be check through a brute force calculation.)

This illustrates how the proof of weak Mordell-Weil could have been written in a purely elementary way (at least for the case of $E(\mathbb{Q})/2E(\mathbb{Q})$). However, the framework of descent, cohomology, and Selmer groups is much more robust and allows us to do more complicated descent argument that could not be written out by hand.

References

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*. Vol. 201. Graduate Texts in Mathematics. An introduction. Springer-Verlag, New York, 2000, pp. xiv+558. 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 (↑ p. 5).

[Poo17] Bjorn Poonen. *Rational points on varieties*. Vol. 186. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2017, pp. xv+337. ISBN: 978-1-4704-3773-2. DOI: 10.1090/gsm/186. URL: https://doi.org/10.1090/gsm/186 (↑ p. 1).