# REVERSE ENGINEERED DIOPHANTINE EQUATIONS

STEVAN GAJOVIĆ

Abstract. We answer a question of Samir Siksek, asked at the open problems session of the conference “Rational Points 2022”, which, in a broader sense, can be viewed as a reverse engineering of Diophantine equations. For any finite set $S$ of perfect integer powers, using Mihăilescu’s theorem, we construct a polynomial $f_S \in \mathbb{Z}[x]$ such that the set $f_S(\mathbb{Z})$ contains a perfect integer power if and only if it belongs to $S$. We first discuss the easier case where we restrict to all powers with the same exponent. In this case, the constructed polynomials are inspired by Runge’s method and Fermat’s Last Theorem. Therefore we can construct a polynomial-exponential Diophantine equation whose solutions are described in advance.

**Key words:** Diophantine equations, Fermat’s Last Theorem, Mihăilescu’s theorem, Runge’s method, elliptic curves

## 1. Introduction

Diophantine problems look innocent but often are tricky. They can be formulated using very basic mathematics, but it turns out that solving many of them took centuries of serious work by numerous mathematicians. Some of them are still not solved; they are famous conjectures in mathematics and, more precisely, in number theory.

The most famous Diophantine equations include some relations with perfect integer powers, and we briefly survey them in §2.1. We will use some of these equations in the main results of this paper in §3.2 and §4.

When we also include rational solutions, to simplify the notation, we will talk about Diophantine problems. We also mention in §2.2 one instance of famous Diophantine problems, classifying the set of rational points $C(\mathbb{Q})$ on curves $C$ defined over $\mathbb{Q}$. We briefly use some of the results and techniques mentioned there in §3.2.

In §2, we note that Diophantine problems are an active and very challenging area of mathematics. On the other hand, there are equations that are trivial to solve, such as linear Diophantine equations, or some equations that have obvious ways to be solved, e.g., by considering them modulo $n$ for some $n \in \mathbb{Z}_{>1}$, or, more generally, using local obstructions.

Therefore, it is an interesting problem to look into the middle case - can we create similar Diophantine equations with a prescribed set of solutions so that we can solve them more easily, but not that obviously? The main task of this article is to take a different perspective - and construct Diophantine equations of a specific shape with a described set of solutions. That was precisely the question Samir Siksek asked during the conference “Rational Points 2022”. Namely, if we consider a Diophantine equation of the type

$$f(x) = y^n,$$

for a given $f \in \mathbb{Z}[x]$, with unknowns $x, y, n \in \mathbb{Z}$ and $n \geq 2$, can it happen that a triple $(x, y, n)$ is a solution if and only if $y^n$ belongs to a finite set of integer powers given in advance?

### 1.1. Main results.

We now reformulate Siksek’s question and make it more precise. Let

$$\mathcal{P} = \{a^m : a \in \mathbb{Z}, m \geq 2\} \subseteq \mathbb{Z}$$

denote the set of all perfect integer powers.

**Question 1.1** (Siksek). *Let $S \subseteq \mathcal{P}$ be a finite set of perfect powers. Is there a polynomial $f_S \in \mathbb{Z}[x]$ such that $f_S(\mathbb{Z}) \cap \mathcal{P} = S$?*

Here we give an affirmative answer to Question 1.1 by constructing such a polynomial in §4, see Theorem 4.1.

One could ask an easier question. Let $m \geq 2$ be a fixed integer. Denote by $\mathcal{P}_m = \{a^m : a \in \mathbb{Z}\}$ the set of all perfect $m$th powers of integers.

**Question 1.2** (Siksek)**.** *Let $S \subseteq \mathcal{P}_m$ be a finite set of $m$th powers. Is there a polynomial $f_S \in \mathbb{Z}[x]$ such that $f_S(\mathbb{Z}) \cap \mathcal{P}_m = S$?*

We recall that in Question 1.2, we fix $m \in \mathbb{Z}_{\geq 2}$. Curves of the shape $C : y^m = f(x)$ are called *superelliptic curves*. We can also rephrase Question 1.2 as a task to construct superelliptic curves whose integral points have prescribed $y$-coordinates in advance.

We explain two different methods to construct a polynomial as asked for in Question 1.2 (one method only works for $m \geq 3$) in §3.1 and §3.2, see Theorem 3.1 and Corollary 3.3, respectively.

We briefly comment on the same question when integers are replaced by rational numbers in §5. We note that one of two approaches to solving Question 1.2 still works over rationals, as explained in §5.1. However, our approach for Question 1.1 does not extend to rational numbers; but in the meantime, Question 5.2 was solved by Santicola [20] by clever and precise refining of the arguments presented here, see §5.2.

## 2. Famous Diophantine problems

2.1. **Famous Diophantine equations.** Now we present several famous Diophantine equations or related conjectures. We also mention the time needed to solve these equations. We recall that these equations mentioned below ask for or are related to integer solutions.

(1) *Fermat's Last Theorem*: $x^n + y^n = z^n$, with an integer $n \geq 3$. It took more than 350 years until it was proven in series of papers by Wiles et al. that this equation has only trivial solutions, i.e., such that $xyz = 0$.

(2) *Generalized Fermat's Equation*: $x^k + y^l = z^m$, where $k, l, m \geq 2$ are integers, see [2] for more details. A special case of this equation is related to the *Beal conjecture* which states that if

$$k, l, m \geq 3,$$

then for any solution $(x, y, z) \in \mathbb{Z}^3$, there is a prime number $p$ such that $p \mid x$, $p \mid y$, $p \mid z$, i.e., solutions cannot be triples of coprime integers. Note that the condition that $k, l, m \geq 3$ is necessary, as otherwise one can find coprime solutions, such as $1^k + 2^3 = (\pm 3)^2$, for any $k \geq 2$, or, for example, $2^5 + 7^2 = 3^4$. More identities can be found in [2].

For fixed $k, l, m \geq 2$ such that

$$1/k + 1/l + 1/m < 1,$$

Darmon and Granville [6] proved that there are only finitely many triples of coprime integers $(x, y, z)$ such that $x^k + y^l = z^m$.

If we vary $k, l, m \geq 2$ such that $1/k + 1/l + 1/m < 1$, there is a conjecture, the *Fermat–Catalan conjecture*, stating that there are only finitely many sextuples

$$(x, y, z, k, l, m)$$

such that $x^k + y^l = z^m$ and $x, y, z$ are coprime.

(3) Former *Catalan's conjecture*, now *Mihăilescu's theorem*: The equation $x^a - y^b = 1$ with integers $a, b \geq 2$ and $x, y > 0$ has only one solution $3^2 - 2^3 = 1$. In other words, the only two positive integers which are consecutive perfect powers of integers are 8 and 9. This statement was conjectured by Catalan and proved by Mihăilescu [14] slightly more than 150 years later.

(4) *(Generalized) Ramanujan-Nagell equation*: The Ramanujan-Nagell equation is the equation $x^2 + 7 = 2^n$, where $x$ and $n$ are integers. Ramanujan conjectured that there are five values of $n$ for which the equation has a solution, $n \in \{3, 4, 5, 7, 15\}$, and Nagell proved this 35 years later. It was first published in Norwegian, and later in English [18]. The generalized Ramanujan-Nagell equation is an equation of the shape $x^2 + D = y^n$, where $x, n, D \in \mathbb{Z}$ and $n \geq 3$. It is widely studied, for example, see [5], or [11] for a recent survey on this equation. Note that some authors, such as, in [16], consider the slightly different equation $F(x) = p_1^{e_1} \cdots p_s^{e_s}$, for some $F \in \mathbb{Z}[x]$ and $p_1, ..., p_s$ prescribed primes and $e_i \geq 0$ (unknown) exponents.

2.2. **Rational points on curves.** One of the most important examples of Diophantine problems is the following trichotomy of rational points on curves defined over $\mathbb{Q}$ (and in fact, over any number field $K/\mathbb{Q}$). Let $C/\mathbb{Q}$ be a *nice* curve; here, the adjective *nice* is a well-known notation used for a smooth, projective, and geometrically irreducible curve. Denote the genus of $C$ by $g(C)$.

(a) (*known for a long time*) If $g(C) = 0$, then either $C(\mathbb{Q}) = \emptyset$ (e.g., consider $C : x^2 + y^2 = 3$) or $C(\mathbb{Q})$ is infinite (e.g., consider $C : x^2 + y^2 = 1$, this curve can be used to parametrize the Pythagorean triples) and furthermore isomorphic to $\mathbb{P}^1(\mathbb{Q})$.

(b) (*Mordell, 1922* [15]) If $g(C) = 1$ and $C(\mathbb{Q}) \neq \emptyset$, then $C$ is called an *elliptic curve* and there is a group law on $C(\mathbb{Q})$, which makes $C(\mathbb{Q})$ a finitely generated group, i.e., $C(\mathbb{Q}) \cong \mathbb{Z}^r \bigoplus T$, where $T$ is a finite (torsion) subgroup, and $r$ is called the *rank* of $C$ over $\mathbb{Q}$.

There are only finitely many possibilities for the torsion subgroup $T$ (exactly 15), as these were classified by Mazur [12], [13]. To prove this statement, Mazur determined rational points on certain types of curves, called modular curves.

Computing the rank $r$ is still a difficult problem, and there are some ways that might succeed in computing it, but there is still no guarantee that the known algorithms can compute the rank of all elliptic curves, look, for example, at Silverman's book [23]. Also, these algorithms for computing ranks are quite complicated, and in practice, it is challenging for humans to perform them. Hence, these algorithms are implemented in computer algebra systems, such as `Magma` [3].

(c) (*Faltings, 1983* [8]) If $g(C) \geq 2$, then $C(\mathbb{Q})$ is finite. In [15], Mordell conjectured this statement, so it took about 60 years until it was proved. This statement was so difficult and significant that Faltings won a Fields medal for this proof. By now, there are a few different proofs of this statement.

However, there are no practical algorithms to compute $C(\mathbb{Q})$ for a given curve $C$, and it is a very active area of research to find methods that can compute precise sets of rational points on curves. As we have already seen in the case of elliptic curves, there are significant problems that reduce to computing rational points on curves (e.g., Mazur's theorem), so it is indeed very important nowadays to further develop existing methods for determining rational points on curves.

Unlike elliptic curves, the set $C(\mathbb{Q})$ for $g(C) \geq 2$ has no particular algebraic structure, so sometimes we want to study it by embedding it into an object with more structure, called the *Jacobian* $J$ of the curve $C$; this is an abelian variety. As for elliptic curves, Weil [26] in 1929 proved, now called Mordell-Weil theorem, that $J(\mathbb{Q})$ is a finitely generated abelian group, i.e., $J(\mathbb{Q}) \cong \mathbb{Z}^r \bigoplus T$, where $T$ is a finite (torsion) subgroup and $r$ is called the *rank* of $J$. In contrast to elliptic curves, much less is known about possibilities for $T$, and the computation of $r$ is much more difficult. In some cases, there are ways to do so, for example, for Jacobians of hyperelliptic curves, by Stoll [25], which is implemented in `Magma`.

## 3. The same exponent

Fix $m \geq 2$. Let $S = \{a_1^m, \ldots, a_k^m\}$ be a set of $k$ distinct $m$th powers of integers $a_1, \ldots, a_k$. We now construct a polynomial $f_S \in \mathbb{Z}[x]$ such that $f_S(\mathbb{Z}) \cap \mathcal{P}_m = S$.

3.1. **First approach.** The solution is inspired by Runge's method (invented in 1887 by Runge [19]; see [21, Chapter 5] for a nice survey). We first define an auxiliary polynomial

$$g(x) = (x - a_1) \cdots (x - a_k).$$

Consider a polynomial

$$f_S(x) = (x(x^2 + 1)g(x))^{4m} + (x^{2m} - x^2 + 2)g(x)^{2m} + x^m.$$

**Theorem 3.1.** *We have*

*(i)* $S \subseteq f_S(\mathbb{Z}) \cap \mathcal{P}_m$*;*

*(ii)* $f(x) \notin \mathcal{P}_m$ *for any* $x \in \mathbb{Z} \setminus \{0, a_1, \ldots, a_k\}$*;*

*(iii)* $f_S(\mathbb{Z}) \cap \mathcal{P}_m = S$*.*

*Proof.*

(i) We evaluate (note that this statement is true regardless whether $a_1 \cdots a_k = 0$ or not)

$$f_S(0) = 2(a_1 \cdots a_k)^{2m}, \quad g(a_i) = 0, \quad f_S(a_i) = a_i^m, \quad \text{for } 1 \leq i \leq k.$$

(ii) Let $x \in \mathbb{Z} \setminus \{0, a_1, \dots, a_k\}$. We first note that $|g(x)| = |(x-a_1)\cdots(x-a_k)| \geq 1$. Then

$$(x^{2m} - x^2 + 2)g(x)^{2m} \geq x^{2m} - x^2 + 2 \geq x^{2m} - |x|^m + 2 > |x|^m.$$

It follows that $(x^{2m} - x^2 + 2)g(x)^{2m} + x^m > 0$, so

$$f_S(x) > (x(x^2+1)g(x))^{4m} = ((x(x^2+1)g(x))^4)^m.$$

Now we prove that

$$f_S(x) < ((x(x^2+1)g(x))^4 + 1)^m, \tag{1}$$

implying that $f(x)$ cannot be an $m$th power because it is nested between two consecutive $m$th powers. To prove inequality (1), it suffices to show

$$m(x(x^2+1)g(x))^{4m-4} > (x^{2m} - x^2 + 2)g(x)^{2m} + x^m. \tag{2}$$

The following two inequalities will help us to show (2). The first one is

$$(x(x^2+1)g(x))^{4m-4} > (x^{2m} - x^2 + 2)g(x)^{2m} \tag{3}$$

which holds because $g(x)^{4m-4} \geq g(x)^{2m}$ and the inequality

$$(x(x^2+1))^{4m-4} > x^{2m} - x^2 + 2$$

is trivial (note that $x \neq 0$).

The second one is clear

$$(x(x^2+1)g(x))^{4m-4} \geq (x(x^2+1))^{4m-4} > |x|^m \geq x^m. \tag{4}$$

Inequality (2) follows from $m \geq 2$ and inequalities (3) and (4).

(iii) Follows directly from (i) and (ii).

□

3.2. **Second approach.** If $m \geq 3$, there is another way to construct the required polynomial $f_S \in \mathbb{Z}[x]$. The term $(x^{2m} - x^2 + 2)((x-a_1)\cdots(x-a_k))^{2m}$ in the previous construction was used to ensure that $f(0)$ in not an $m$th power if $a_1 \cdots a_k \neq 0$. One could try a simpler construction

$$g_S(x) = ((x-a_1)\cdots(x-a_k))^m + x^m.$$

By Fermat's Last Theorem, $g_S(x)$ is not an $m$th power unless $x \in \{0, a_1, \dots, a_k\}$. However, we want to exclude the possibility for $x = 0$ if $a_1 \cdots a_k \neq 0$. We instead use a more general Fermat's Equation, as suggested by Samir Siksek. Consider

$$f_S(x) = 3((x-a_1)\cdots(x-a_k))^m + x^m.$$

**Lemma 3.2.** *Let $m \geq 3$. If $(x_1, x_2, x_3) \in \mathbb{Z}^3$ satisfy $3x_1^m + x_2^m = x_3^m$, then $x_1 = 0$.*

*Proof.* We distinguish three cases according to whether $m$ has a prime divisor $p \geq 5$, $m$ is a power of 3, or $m \geq 4$ is a power of 2.

(i) Let $p \geq 5$ be a prime number dividing $m$. By a generalized approach to Fermat's Last Theorem by Kraus [10], the equation $3x_1^p + x_2^p = x_3^p$ has only trivial solutions $x_1x_2x_3 = 0$, which implies that $x_1 = 0$. See also notes by Siksek [24] for a nice explanation of the modular method. In this concrete case, see [24, Theorems 1, 15] for an argument that a non-trivial solution to $3x_1^p + x_2^p = x_3^p$ corresponds to a certain newform of weight 2 and level 6, which does not exist. Hence, if $3x_1^m + x_2^m = x_3^m$, then $x_1 = 0$.

(ii) If $m$ is a power of 3, it suffices to consider $m = 3$. The cubic curve

$$X\colon 3x_1^3 + x_2^3 = x_3^3$$

has genus one and $X(\mathbb{Q}) \neq \emptyset$, hence it is isomorphic over $\mathbb{Q}$ to an elliptic curve. As pointed out in §2.2 (b), using `Magma` [3], we prove that the rank of $X$ is zero, and that $X(\mathbb{Q})$ consists only of the point at infinity, which corresponds precisely to $x_1 = 0$.

(iii) If $m \geq 4$ is a power of 2, it suffices to consider $m = 4$. Integral solutions to $3x_1^4 + x_2^4 = x_3^4$ correspond to the rational points on a curve

$$X'\colon 3x^4 + y^4 = 1.$$

One can consider a curve

$$X/\mathbb{Q}\colon y^2 = 1 - 3x^4.$$

As we stated in §2.2 (c), we can embed $X$ into its Jacobian $J$, and, using `Magma`, we prove $J(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. Hence, we conclude $\#X(\mathbb{Q}) \leq \#J(\mathbb{Q}) = 2$, so $X(\mathbb{Q}) = \{(0, \pm 1)\}$, implying $X'(\mathbb{Q}) = \{(0, \pm 1)\}$, and hence, that $x_1 = 0$.

□

**Corollary 3.3.** *We have $f_S(\mathbb{Z}) \cap \mathcal{P}_m = S$.*

*Proof.* It follows by Lemma 3.2 that $f_S(x) \in \mathcal{P}_m$ only when $x \in S$, and we compute directly that $f_S(a_i) = a_i^m$ for every $1 \leq i \leq k$. □

We note that this approach does not work directly for $m = 2$ as the equation

$$qx_1^2 + x_2^2 = x_3^2$$

has solutions with $x_1 \neq 0$ for any $q \in \mathbb{Z}$. We may assume that $q > 0$. If $q$ is not a square of an integer, then, consider $x_2 = 1$ and note that Pell's equation $x_3^2 - qx_1^2 = 1$ has infinitely many solutions. If $q = r^2$ is a square of an integer $r$, then $(rx_1, x_2, x_3)$ is a Pythagorean triple, and we can find infinitely many of them (for example, let $x_1 = 2s$, $x_2 = s^2 - r^2$, $x_3 = s^2 + r^2$, for $s \in \mathbb{Z}$).

## 4. General case

In this section, using Mihăilescu's theorem, we construct a polynomial with the desired property in the general case. Let $S = \{b_1, \ldots, b_k\} \subseteq \mathcal{P}$ be a finite set of perfect integer powers. We construct a polynomial $f_S \in \mathbb{Z}[x]$ such that $f_S$ is the identity on $S$, and $f_S(x) \notin \mathcal{P}$, for all $x \in \mathbb{Z} \setminus S$. Define an auxiliary polynomial

$$g(x) = ((x - b_1) \cdots (x - b_k))^4 + 1,$$

and let

$$f_S(x) = g(x)((x - 1)g(x) + 1).$$

We now prove that $f_S$ satisfies the property asked in Question 1.1, hence giving a positive answer to Question 1.1.

**Theorem 4.1.**

*(i) Let $x \in \mathbb{Z}$. Then $f_S(x) \in \mathcal{P}$ if and only if $x \in S$.*
*(ii) We have $f_S(\mathbb{Z}) \cap \mathcal{P} = S$.*

*Proof.*

(i) Let $x \in \mathbb{Z}$ be such that $f_S(x) = y^n$, for some integers $y, n$ with $n \geq 2$. Since $g(x)$ and $(x - 1)g(x) + 1$ are coprime integers, we conclude that there is $z \in \mathbb{Z}$ such that $g(x) = \pm z^n$, and since $g(x) > 0$, we may assume that $g(x) = z^n$. Denote

$$c := (x - b_1) \cdots (x - b_k).$$

Then we have

$$z^n - c^4 = 1.$$

Since the exponent of $c$ is greater than 3, by Mihăilescu's theorem, the only possibility is that $z = 1$ and $c = 0$, implying that $x = b_i$ for some $1 \leq i \leq k$. If $x \in S$, we evaluate $f_S(x) = x \in \mathcal{P}$.

(ii) Follows from (i) and the fact that $f_S$ is the identity on $S$.

□

## 5. Generalizations.

It is interesting to see whether our approaches work when we ask the same questions with integers replaced by rational numbers. Denote by $\mathcal{Q} = \{a^m \colon a \in \mathbb{Q}, m \geq 2\}$ the set of all rational powers, and, for a fixed integer $m \geq 2$, let $\mathcal{Q}_m = \{a^m \colon a \in \mathbb{Q}\}$ be the set of all $m$th powers of rational numbers. We have naturally two questions.

### 5.1. Rational numbers: The same exponent.

**Question 5.1.** *Let $S \subseteq \mathcal{Q}_m$ be a finite subset of mth rational powers. Is there a polynomial $f_S \in \mathbb{Q}[x]$ such that $f_S(\mathbb{Q}) \cap \mathcal{Q}_m = S$?*

We first note that for $m \geq 3$ we can give a positive answer to Question 5.1. It is clear that the first approach cannot be used because there is no version of Theorem 3.1 that covers rational numbers. In this approach, we use the property that distinct integers differ by at least 1, which is not true for rational numbers; their absolute difference can be arbitrarily small. However, Lemma 3.2 remains true for rational numbers, i.e., if we replace the condition $(x_1, x_2, x_3) \in \mathbb{Z}^3$ by $(x_1, x_2, x_3) \in \mathbb{Q}^3$. This follows because the equation $3x_1^m + x_2^m = x_3^m$ is homogeneous, so any rational solution easily leads to an integer solution. Hence, if $S = \{a_1^m, \dots, a_k^m\}$ is a set of $k$ distinct $m$th powers of rational numbers $a_1, \dots, a_k$, where $m \geq 3$, then again, for the polynomial

$$f_S(x) = 3((x - a_1) \cdots (x - a_k))^m + x^m,$$

we have that $f_S(\mathbb{Q}) \cap \mathcal{Q}_m = S$.

### 5.2. Rational numbers: General case.

On the other hand, the approach from §4 does not work directly over rational numbers. We cannot use the coprimality argument in the factorization so easily; we would need to take care of possible denominators. Hence, we can formulate the question:

**Question 5.2.** *Let $S \subseteq \mathcal{Q}$ be a finite set of perfect rational powers. Is there a polynomial $f_S \in \mathbb{Q}[x]$ such that $f_S(\mathbb{Q}) \cap \mathcal{Q} = S$?*

This question was answered affirmatively by Santicola [20], who noted that it is sufficient to use special cases of Mihăilescu's theorem proven by Lebesgue [9] to answer Question 1.2. Furthermore, Santicola's construction uses the results of [1, 4, 7]. To handle possible denominators and to prove the key lemma [20, Lemma 6], Santicola used the result of Pethő [17], and independently of Shorey and Stewart [22].

### 5.3. Challenge.

We see that this article has already inspired further research. It is also interesting to consider this question over other rings and fields. We challenge the interested reader to try to answer the analogous questions over $\mathbb{Z}[i]$ or $\mathbb{Q}[i]$, or, in general, over $\mathcal{O}_K$ or $K$, where $K/\mathbb{Q}$ is any number field.

**Acknowledgment.** The author would like to thank Samir Siksek for raising the questions, discussing the topic and giving useful comments and suggestions, Michael Stoll for organizing the conference "Rational Points 2022" and for the financial support for the conference, Ludwig Fürst and Himanshu Shukla for conversations about this topic and writing a report on the problem session, and Pieter Moree, Oana Padurariu, and Alain Togbe for many valuable comments that improved the article. The author was supported by a guest postdoc fellowship at the Max Planck Institute for Mathematics in Bonn, by Czech Science Foundation GAČR, grant 21-00420M, and by Charles University Research Centre program UNCE/SCI/022 during various stages of this project.

## References

[1] Bennett, M. and Ellenberg, J. S. and Ng, N. (2010). The Diophantine Equation $A^4 + 2^\delta B^2 = C^n$, International Journal of Number Theory. 06: 311–338.

[2] Bennett, M. and Mihăilescu, P. and Siksek, S. (2016). The generalized Fermat equation. Open problems in mathematics: Springer, [Cham]. 173–205.

[3] Bosma, W. and Cannon, J. and Playoust, C. (1997). The Magma algebra system. I. The user language. Journal of Symbolic Computation. 24(3–4): 235–265.

[4] Bruin, N. (1999). The Diophantine Equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. Compositio Mathematica. 118(3): 305–321.

[5] Bugeaud, Y. and Mignotte, M. and Siksek, S. (2006). Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation. Compositio Mathematica. 142(1): 31–62.

[6] Darmon, H. and Granville, A. (1995). On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. The Bulletin of the London Mathematical Society. 27(6): 513–543.

[7] Ellenberg, J. S. (2004). Galois Representations Attached to $\mathbb{Q}$-Curves and the Generalized Fermat Equation $A^4 + B^2 = C^p$. American Journal of Mathematics. 126(4): 763–787.

[8] Faltings, G. (1983). Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Inventiones Mathematicae. 73(3): 349–366.

[9] Lebesgue, V. A. (1850). Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + I$. Nouvelles annales de mathématiques : journal des candidats aux écoles polytechnique et normale 9: 178–181.

[10] Kraus, A. (1997). Majorations effectives pour l'équation de Fermat généralisée. Journal Canadien de Mathématiques. 49(6): 1139–1161.

[11] Le, M. and Soydan, G. (2020). A brief survey on the generalized Lebesgue-Ramanujan-Nagell equation. Surveys in Mathematics and its Applications. 15: 473–523.

[12] Mazur, B. (1977). Modular curves and the Eisenstein ideal, Publications Mathématiques I.H.E.S. 47: 33–186.

[13] Mazur, B. (1977). Rational points on modular curves. In: Serre, JP., Zagier, D.B. (eds) Modular Functions of one Variable V. Lecture Notes in Mathematics, vol 601. Springer, Berlin, Heidelberg. 107–148.

[14] Mihăilescu, P. (2004). Primary cyclotomic units and a proof of Catalan's conjecture. Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]. 572: 167–195.

[15] Mordell, L, J. (1922), On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc. Camb. Phil. Soc. 21: 179–192.

[16] Moree, P. and Stewart, C. L. (1990) Some Ramanujan-Nagell equations with many solutions, Indag. Math. (N. S.) (4) 1: 465–472.

[17] Pethő, A. (1982). Perfect powers in second order linear recurrences. Journal of Number Theory. 15(1): 5–13.

[18] Nagell, T. (1961). The diophantine equation $x^2 + 7 = 2^n$. Arkiv för Matematik. Journal Canadien de Mathématiques. 4: 185–187.

[19] Runge, C. (1887). Ueber ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen. Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]. 100: 425–435.

[20] Santicola, K. (2022). Reverse engineered Diophantine equations over $\mathbb{Q}$. Journal de Théorie des Nombres de Bordeaux, to appear.

[21] Schoof, R. (2008). Catalan's Conjecture. Springer-Verlag London, Ltd., London.

[22] Shorey, T. N. and Stewart, C. L. (1983). On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences. Mathematica Scandinavica 52(1): 24–36.

[23] Silverman, J. H. (2009), The arithmetic of elliptic curves, 2nd edition. Springer: Graduate Texts in Mathematics. Volume 106.

[24] Siksek, S. (2016). The Modular Approach to Diophantine Equations, `http://homepages.warwick.ac.uk/~maseap/sarajevo/notes.pdf`. (accessed 18 May 2022)

[25] Stoll, M. (2001). Implementing 2-Descent for Jacobians of Hyperelliptic Curves. Acta Arithmetica. 98(3): 245–277.

[26] Weil, A. (1929). L'arithmétique sur les courbes algébriques, Acta Mathematica. 52(1): 281–315.