A tour through some Diophantine equations

by **Ariel Pacetti**[*],[**]

Abstract.—The purpose of this short note is to present some results regarding the study of Diophantine equations, ranging from very old problems (well known results to most mathematicians) to some quite new results in the area. Most of the times, the techniques developed to solve particular problems are more interesting than the results themselves. The last section contains our humble contribution.

1 Introduction

The term *Diophantine equations* comes from the pioneer work of Diophantus of Alexandria, a Greek mathematician that lived sometime around 200 AD. In a series of books called *Arithmetica*, Diophantus studied solutions (over the positive rational numbers) to different systems of equations. In this short article we will mostly focuses on studying (integral or rational) solutions of a single equation of the form

$$F(x,y)=0,$$

for some polynomial $F(x,y)$ with integral coefficients.

2 Linear Diophantine Equations

Let a,b,c be three rational integers, with the condition that the pair (a,b) is not $(0,0)$. Consider the equation

$$aX+bY=c. \tag{1}$$

The set of solutions to (1) form a line, and it is well known that it has infinitely many rational points. However, it is not so clear what happens with its set of integral points. For example, the line

$$2X+2Y=1,$$

does not have any integral point (the reason being that the left hand side is always even, while 1 is odd). Similarly, for (1) to have an integral solution, it must be the case that any number dividing a and b must also divide c. It is not hard to prove that this condition is enough for the existence of solutions.

Theorem 1.— The equation (1) has an integral solution if and only if $\gcd(a,b)\mid c$. Furthermore, if it has one, it has infinitely many.

Proof.— See §5 of the very nice book [11]. ∎

Actually the proof is constructive: suppose that $\gcd(a,b)\mid c$. Using the Euclidean algorithm, one can construct integers r,s such that

$$\gcd(a,b)=a\cdot r+b\cdot s.$$

Multiplying both sides by $\frac{c}{\gcd(a,b)}$ gives a non-trivial solution $x_0=\frac{rc}{\gcd(a,b)}$, $y_0=\frac{sc}{\gcd(a,b)}$. Then all solutions are of the form

$$\begin{cases} x=x_0+\kappa\frac{b}{\gcd(a,b)},\\ y=y_0-\kappa\frac{a}{\gcd(a,b)}.\end{cases}$$

for $\kappa\in\mathbb{Z}$. It is important to remark that computing integral solutions is much harder than finding the rational ones.

[*] CIDMA, University of Aveiro. Email: apacetti@ua.pt

[**] Aknowledgements: This work was supported by CIDMA and is funded by the Portuguese Foundation for Science and Technology,.under grant UIDB/04106/2020 (https://doi.org/10.54499/UIDB/04106/2020)

3 Conics

Consider now the case of a degree two polynomial in the variables x, y, namely a polynomial of the form

$$aX^2 + bXY + cY^2 + dX + eY + f = 0, \qquad (2)$$

where we can assume that a, b, c, d, e, f are all integers (otherwise we can multiply by the minimum common multiple of their denominators). We will also assume that the degree two polynomial is irreducible (i.e. is not the product of two degree 1 ones), as otherwise the study of its rational/integral points reduces to the study of points on the factors.

We start studying rational solutions, say of the form $(X/Z, Y/Z)$ where X, Y, Z are integers. Substituting in (2) and multiplying by Z^2, we obtain an integral point on the *projective* conic

$$aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0, \quad (3)$$

where $Z \neq 0$ (it is customary to consider solutions where at least one of the coordinates is non-zero, as they correspond to points in the projective plane).

A general conic like (3) might not have integer solutions for easy reasons, for example there are no solutions to the equation $X^2 + Y^2 + Z^2$ other than $(0, 0, 0)$ (which we do not consider). In this case, the failure for a solution to exist comes from the fact that there are no real solutions to it (this is called an *Archimedean* failure). There might be other failures.

Example 1.— The conic $X^2 + Y^2 = 3Z^2$ has no non-trivial solution.

Suppose it does have a non-trivial solution (a, b, c) and assume that $\gcd(a, b, c) = 1$ (otherwise, we can divide each a, b, c by $\gcd(a, b, c)$ obtaining a new solution with this property). Note that if we divide any square by 4, the remainder is either 0 or 1 (or in terms of congruences, $x^2 \equiv 0, 1 \pmod 4$). Then $a^2 + b^2$ while divided by 4 has reminder 0, 1 or 2. Note that it is zero precisely when $2 \mid a$ and $2 \mid b$. Similarly, the reminder of $3c^2$ while divided by 4 is 0 or 3. Then the equality $a^2 + b^2 = 3c^3$ implies that both sides are divisible by 4, so $2 \mid c$ as well, contradicting the assumption that $\gcd(a, b, c) = 1$.

Contrary to the previous example, now the failure has to do with the prime 2, it is what is called a 2-adic failure (related to non-existence of solutions over the field $\mathbb{Q}_2$ of 2-adic numbers). A similar obstruction appears for the prime $p = 3$ (we leave the details to the reader).

It is natural to wonder whether the non-existence of solutions is always due to a *local* (i.e. attached to a congruence modulo N for some integer N) or an Archimedean reason. Indeed this is the case.

Theorem 2 (Hasse-Minkowski).— An equation like (3) has a non-zero rational solution if and only if it has a real solution, and a solution modulo N for all positive integers N.

Proof.— See for example Theorem 8 in [15]. ∎

The proof presented by Serre is different from our statement, so let us add a few comments. By the Chinese remainder Theorem (see §2.3 of [11]), searching for solutions modulo a general integer N is equivalent to search for solutions modulo prime powers. Once the prime p is fixed, the existence of a solution modulo p^n for all positive integers n is equivalent to the existence of a solution over the field of p-adic numbers. This is what Serre proves in [15].

Remark 1.— The result of Hasse-Minkowski works for homogeneous polynomials of degree 2 in any number of variables (not just 3).

Remark 2.— As stated Theorem 2 seems only of a theoretical nature (as it implies verifying infinitely many conditions). However, it is easy to transform it into a finite computation (it is enough to verify the statement at primes dividing the discriminant of the quadratic form together with the case $p = 2$). See for example §5.4 of [4].

Once that we have an *algorithm* to determine whether a conic has a rational point or not, it is natural to ask how many rational points it might have. The answer is infinitely many, as a conic with a point is isomorphic to a line, as proved in the following example.

Example 2.— Let us study the case of the unit circle centered at $A = (0, 0)$ with equation

$$\mathscr{C} : X^2 + Y^2 = 1. \qquad (4)$$

Take the point $B = (1, 0)$ (which belongs to the circle). Take the tangent line at B and translate it by some non-zero rational number (for example one to the right as in Figure 1).

Call the line L. Then we get a bijective map from rational points on $\mathscr{C}$ (removing the point B) to rational points on L as follows: given a rational point C in L, consider the line going through C and B. It must intersect the circle $\mathscr{C}$ in a rational point (why?). Explicitly, if $C = (2, y)$ then the second intersection point has coordinates

$$\left(\frac{y^2-1}{y^2+1}, \frac{-2y}{y^2+1}\right). \qquad (5)$$

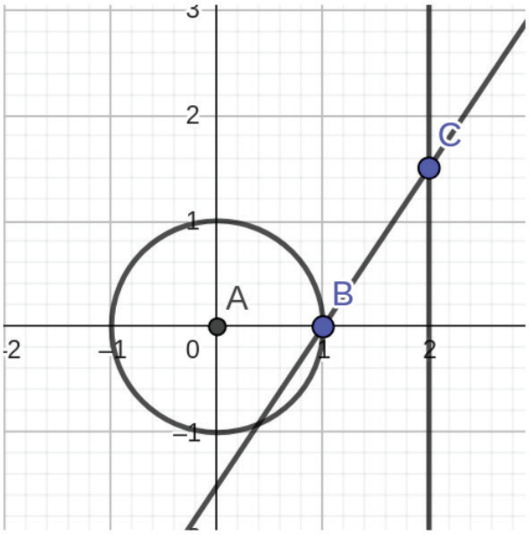

Figure 1.—Rational points circle

The inverse sends a point (x, y) in $\mathscr{C}$ to the point $(2, y/(x-1))$. The reason we need to remove the point B is that the affine line is not compact, if we add its point at infinity, then we really get a bijection between the two sets.

As done with the general equation (2), the set of rational points on the unit circle is the same as the set of integral points on the projective curve $X^2+Y^2 = Z^2$ (the so called Pitagorean triples). Writing the rational point y of the line L in the form $y = \frac{m}{n}$ (for $m, n \in \mathbb{Z}$) we recover the classical parametrization of the Pitagorean triples

$$(m^2 - n^2, -2mn, m^2 + n^2). \tag{6}$$

Remark 3.— The same construction/strategy works for a general conic as in (3) with one rational point.

Remark 4.— Over an algebraically closed field, equation (2) always has a point, hence it is isomorphic to a line. From a topological point of view, a line and a conic are the same, they both are genus 0 curves (or equivalently Riemann surfaces with no holes).

The problem of determining the set of integral points on a conic is much harder. There might be no points at all (as in Example 1), there might be finitely many (for example it is easy to verify that the circle (4) only has the four integral points $\{(\pm 1, 0), (0, \pm 1)\}$) or there might be infinitely many. For example, let d be a square-free positive integer, and consider Pell's equation

$$X^2 - dY^2 = 1. \tag{7}$$

The equation has infinitely many integral solutions, and all of them (up to a sign) can be obtained as *powers* of a particular one (see for example §7.8 of [11]). This equation appears while studying the *integers* whose inverses are also integers in the quadratic field $\mathbb{Q}(\sqrt{d})$.

4 Cubics

As mentioned before, we are mostly interested in studying hypersurfaces, i.e. solutions of a single equation $F(x_1, \dots, x_n) = 0$ (furthermore, most of the time we restrict to $n = 2$). The hypersurface

$$\mathscr{C} : F(x_1, \dots, x_n) = 0$$

is *non-singular* (or smooth) is there are no points P in $\mathscr{C}$ satisfying that $\frac{\partial F}{\partial x_i}(P) = 0$ for all $i = 1, \dots, n$. All lines are smooth, and conics given by an irreducible polynomial are smooth as well.

Suppose that $F(x, y)$ is a cubic (i.e. it has degree 3), and that the curve

$$\mathscr{C} : F(x, y) = 0$$

is non-singular. How can we determine whether it has a rational point or not?

As happened before, it is better to work with an homogeneous polynomial $F(X, Y, Z)$ in 3 variables. Its set of solutions corresponds to a cubic in the projective plane, and we are trying to determine whether it has an integral point different from $(0, 0, 0)$.

The first approach would be to use Hasse's criterion, i.e. try to search for points modulo N for different values of N. If no such a point exists, then we have proved that the curve $\mathscr{C}$ has no rational points.

Theorem 3 (Selmer).— The cubic equation

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

has the only solution $(0, 0, 0)$ over $\mathbb{Q}$, but it has a nonzero solution over $\mathbb{R}$ and modulo N for all N.

Proof.— See [14]. ∎

Selmer's example shows that Hasse-Minkowski result does not hold for degrees larger than 2. Let us state some very interesting density results.

Theorem 4.— The probability that a random plane cubic curve over $\mathbb{Q}$ has a point modulo N for all positive values of N is approximately 97.256%

Proof.— See Theorem 2 of [2]. ∎

Remark 5.— Unlike conics, a cubic polynomial always has a real root, so the only failures can be local ones.

Furthermore, it was proved by Bhargava (see https://arxiv.org/pdf/1402.1131.pdf) that a positive proportion of cubics (at least 28%) fail the Hasse principle, so another approach is needed.

Assuming a deep open conjecture (namely finiteness of the Tate-Shafarevich group), there does exist an algorithm to determine if a cubic has a rational point or not. In practice, running the algorithm in some particular bad behaved cases might be very challenging.

Definition 5.— An *elliptic curve* is a non-singular cubic with a rational point.

The usual definition of an elliptic curve is that of a non-singular genus 1 curve with a rational point. It is not hard to prove (see for example §III.3 of [17]) that any rational elliptic curve can be given by a Weierstrass equation

$$E : Y^2 = X^3 + AX + B, \tag{8}$$

for $A, B \in \mathbb{Q}$ with $4A^3 + 27B^2 \neq 0$ (so the curve is smooth). The marked rational point corresponds to the solution $O = (0 : 1 : 0)$ of the homogeneous polynomial

$$ZY^2 = X^3 + AXZ^2 + BZ^3.$$

The point O is the unique point at the infinity line which we do not see while working on the affine plane.

Elliptic curves are very interesting objects. If K is any field (like $\mathbb{Q}$ or $\mathbb{C}$), the set $E(K)$ of points on E defined over K has an addition law (see §III.2 of [17]), making $(E(K), +)$ an abelian group (whose identity element is the point O).

Theorem 6 (Mordell).— The group $E(\mathbb{Q})$ is finitely generated.

A proof is given in §VIII of [17]. In particular, the fundamental theorem of finitely generated abelian groups implies that there exists a non-negative integer r such that

$$E(\mathbb{Q}) \simeq T \times \mathbb{Z}^r,$$

where T is a finite group. The number r is called the *rank* of the elliptic curve. There are very effective algorithms to compute T. Furthermore, a conjecture of Beppo Levi proven by Mazur states that there are only 15 possible groups for T (see Theorem 7.5 of [17]). Computing r (and generators for the free part) is a deep problem. Once again, assuming finiteness of the Tate-Shafarevich group, there exists a theoretical algorithm to do it.

Remark 6.— It is not known whether the value of r is bounded or not. The current largest value for it is 28, found by Elkies in 2006.

Regarding integral points, there is a very general result due to Siegel ([16]), which states the following.

Theorem 7.— If $F(x, y)$ is a polynomial of degree larger than 2 and the curve $\mathscr{C} : \{F(x, y) = 0\}$ is non-singular, then $\mathscr{C}$ has finitely many integral points.

The result is not effective (i.e. it does not give information on the number of integral points of $\mathscr{C}$ nor how to compute them). In the case of elliptic curves, the elements of T have integral coordinates. If a set of generators for $E(\mathbb{Q})$ is known then a priori one can determine all the integral points on E.

5 Larger degrees

If the polynomial $F(x, y)$ has degree larger than 3, the (non-singular) curve $\mathscr{C}$ has genus larger than 1. The following result is a deep conjecture of Mordell proven by Falting ([9]).

Theorem 8 (Faltings).— If $\mathscr{C}$ is a rational non-singular curve of genus larger than 1 then $\mathscr{C}(\mathbb{Q})$ is finite.

As Siegel's theorem, the proof is not effective. In a remarkable article, Chabauty ([3]) gave a method to bound the number of rational points when the rank of the Jacobian of $\mathscr{C}$ is smaller than its genus. An effective version of the method was obtained by Coleman in ([6]). Since then, many improvements have been obtained, making the Chabauty method a very active research area.

6 Fermat's last theorem

Without getting into details of the history behind Fermat's last theorem, in a margin of his copy of Diophantus' *Arithmetica*, Fermat wrote that a cube cannot be written as the sum of two cubes, a fourth power as a sum as two fourth powers, etc. In other words, his claim can be stated as:

Theorem 9 (Fermat's last theorem).— The equation

$$X^n + Y^n = Z^n \tag{9}$$

has no rational solutions other than the trivial ones (i.e. when one of the variables equals zero).

After the contributions of many mathematicians, Fermat's last theorem was finally proved in 1995 by Wiles (see [19]). The book [8] contains details of the history behind the problem as well as different strategies used to solve particular cases before the Frey-Hellegouarch approach used in Wiles' proof.

Historically, a major breakthrough for understanding Fermat's last theorem was Faltings' result, which implies the existence of finitely many solutions for each $n > 3$.

The case $n = 3$ is of particular interest, as it is a cubic curve, with a rational point (actually with 3 different ones up to multiplication by -1). Substituting (X, Y, Z) by $(y/9, x/3, y/9z)$ in (9) (when $n = 3$) and multiplying the equation by 27 gives the curve in Weirestrass form

$$y^2z + 9yz^2 = x^3 - 27z^3.$$

Any modern number theory software (like [18]) verifies that this curve has only three rational points, namely $(3 : 0 : 1)$, $(3 : -9 : 1)$ and $(0 : 1 : 0)$ (mapping to the points $(0 : 1 : 1)$, $(-1 : 1 : 0)$ and $(1 : 0 : 1)$ respectively), proving Fermat's last theorem when $n = 3$.

The general proof of Fermat's last theorem is very technical, but we content ourselves to stating a few ingredients of the proof: start with a putative solution (a, b, c) of (9) satisfying that $\gcd(a, b, c) = 1$ and $abc \neq 0$ (to avoid the trivial solutions). It is enough to prove the statement when n is a prime number, and when $n = 4$. The case $n = 4$ was proved by Fermat, so suppose that n is an odd prime number ℓ.

1. Attach to the solution the Frey elliptic curve
$$E : Y^2Z = X(X - a^\ell Z)(X + b^\ell Z).$$
2. Wiles proved that this elliptic curve is *modular* i.e. is related to an holomorphic function of the complex upper half plane satisfying many transformation properties (such functions are called *modular forms*). The number of equations depend on a parameter N (a positive integer) called the *level* of the modular form. For the experienced reader, the modular form has weight 2 and is invariant under the group $\Gamma_0(N)$.
3. For each value of N, the set of modular forms satisfying the relations given by the value N is actually a finite dimensional vector space. There are many algorithms to compute a basis for it (using the so called *modular symbols*). The problem is that the value of N attached to E depends on a, b and c (which are unknown).
4. Making use of the particular shape of a solution, results of Hellegouarch and Ribet imply that actually one can take (up to a congruence) $N = 2$.
5. The space of modular forms for the parameter $N = 2$ is zero, so there is no form in this space to match the curve E attached to our solution. This gives a contradiction, so the original solution (a, b, c) cannot exist.

As previously mentioned, the proof follows from the effort and contributions of many mathematicians, including Frey, Hellegouarch, Mazur, Ribet, Serre, Wiles and Taylor among others.

7 The generalized Fermat equation

Let a, b, c, p, q, r be non-zero positive integers. The so called *generalized Fermat equation* is the equation

$$ax^p + by^q = cz^r. \tag{10}$$

The case $a = b = c = 1$ and $p = q = r$ is the classical Fermat's equation. There is a big difference between equation (10) and Fermat's one, since the former defines an affine surface (instead of a projective curve). There are many examples of surfaces containing lines (like a cone, although it is a singular surface). For this reason, the number of solutions to (10) depends on whether $(1/p) + (1/q) + (1/r)$ is larger than 1, equals 1 or is smaller than 1. See ([1]) for a nice exposition in the case $a = b = c = 1$.

The first case (called spherical) corresponds to the exponents $(2, 2, r)$, $(2, q, 2)$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 4, 3)$ or $(2, 3, 5)$. In general one expects that if one solution exists, then there are infinitely many (and the solutions can be parametrized). See §14 of [5].

The second case (called parabolic) corresponds to the exponents $(2,6,3)$, $(2,4,4)$, $(4,4,2)$, $(3,3,3)$ or $(2,3,6)$. In this cases one also expects that if one solution exists, then there should be infinitely many of them (but we do not expect a parametrization). See §6 of [7] and also §6.5 of [4].

The last case (called hyperbolic) is the general one. Note that since the polynomial giving (10) is not homogeneous, we cannot *assume* that our solution is *primitive* (i.e. $\gcd(x,y,z)=1$). This phenomenom gives raise to the existence of many *unwanted* solutions.

Here is an example taken from [7]: consider the equation

$$x^3+y^3=z^4.$$

(corresponding to equation (10) with parameters $(a,b,c,p,q,r)=(1,1,1,3,3,4)$). Let $z=\alpha^3+\beta^3$, $x=\alpha z$, $y=\beta z$ for α,β arbitrary integers. These are all solutions! (though all of them but finitely many are not primitive). For this purpose, one focus on studying only primitive solutions. Here is a very nice general result.

Theorem 10 (Darmon-Granville).— If $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$ then equation (10) has finitely many primitive solutions.

The proof (see [7]) depends on Mordell's conjecture (Theorem 8), so it is not effective. It is expected that once (a,b,c) is fixed, the set of primitive solutions (where the exponents (p,q,r) vary) is still finite. Here is an explicit version of what we expect to be true.

Conjecture 1.— Any primitive solution to

$$x^p+y^q=z^r,$$

with $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$ is either the solution $1^p+2^3=3^2$, or it belongs to a finite list.

In other words, if we vary the exponents (p,q,r) with the condition that the equation is hyperbolic, then the union of all solutions is a finite set. There is an explicit candidate for the finite list (based on numerical computations) which we omit for space reasons. They all have the property that one of p, q or r equals 2. A conjecture of Beal (with a prize of 1 million USD for its resolution) actually states that there are no solution if $\min\{p,q,r\}>2$.

8 Our contribution to the problem

Together with my former student Lucas Villagra Torcomian, we study the particular generalized Fermat equations:

$$x^4+dy^2=z^p, \qquad (11)$$

and

$$x^2+dy^6=z^p, \qquad (12)$$

for different values of d. In [12], following the modular method used in the proof of Fermat's last theorem, we gave an algorithm that for fixed d, proves (in many instances) the non-existence of solutions for any large value of the exponent p (assuming it is a prime number). Here are a few particular instances of the results proven in [12].

Theorem 11.— There are no non-trivial primitive solutions of $x^4+5y^2=z^p$ if p is any prime number larger than 499.

The result should hold for small values of p as well (say larger than 13), but getting this bound requires a huge computational effort that is unfeasible nowadays.

Theorem 12.— There are no non-trivial primitive solutions of $x^2+6y^6=z^p$ if p is any prime number larger than 563.

When $d<0$ equations (11) and (12) become harder to study. However, in [13] we proved some partial results like the following.

Theorem 13.— Let $p>19$ be a prime number such that $p\neq 97$ and $p\equiv 1,3 \pmod 8$. Then $(\pm 7,\pm 20,1)$ are the only non-trivial primitive solutions of the equation $x^4-6y^2=z^p$.

The aforementioned results depend on a computation for each value of the parameter d. Recently, in [10] we obtained the following asymptotic result.

Theorem 14.— Let d be a prime number congruent to 3 modulo 8 and such that the class number of $\mathbb{Q}(\sqrt{-d})$ is not divisible by 3. Then there are no non-trivial primitive solutions of the equation

$$x^4+dy^2=z^p,$$

for p large enough.

A similar result was obtained for the equation $x^2+dy^6=z^p$, namely that if d is a prime number congruent to 19 modulo 24 and such that the class number of $\mathbb{Q}(\sqrt{-d})$ is not divisible by 3, then the equation $x^2+dy^6=z^p$ does not have non-trivial primitive solutions for p large enough.

References

[1] Michael Bennett, Preda Mihăilescu, and Samir Siksek. The generalized Fermat equation. In *Open problems in mathematics*, pages 173–205. Springer, [Cham], 2016.

[2] Manjul Bhargava, John Cremona, and Tom Fisher. The proportion of plane cubic curves over $\mathbb{Q}$ that everywhere locally have a point. *Int. J. Number Theory*, 12(4):1077–1092, 2016.

[3] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[4] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[5] Henri Cohen. *Number theory. Vol. II. Analytic and modern tools*, volume 240 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[6] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[7] 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.

[8] Harold M. Edwards. *Fermat's last theorem*, volume 50 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. A genetic introduction to algebraic number theory, Corrected reprint of the 1977 original.

[9] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[10] Franco Golfieri Madriaga, Ariel Pacetti, and Lucas Villagra Torcomian. Asymptotic results for the equations $x^4 + dy^2 = z^p$ and $x^2 + dy^6 = z^p$, 2022.

[11] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[12] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-Curves, Hecke characters and some Diophantine equations. *Math. Comp.*, 91(338):2817–2865, 2022.

[13] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-curves, Hecke characters and some Diophantine equations II. *Publ. Mat.*, 67(2):569–599, 2023.

[14] Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85:203–362 (1 plate), 1951.

[15] J.-P. Serre. *A course in arithmetic.* Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.

[16] Carl L. Siegel. Über einige Anwendungen diophantischer Approximationen [reprint of Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1]. In *On some applications of Diophantine approximations*, volume 2 of *Quad./Monogr.*, pages 81–138. Ed. Norm., Pisa, 2014.

[17] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[18] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.13.4*, 2022.Available from http://pari.math.u-bordeaux.fr/.

[19] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.