ON (NON)EXTENSIONS OF FERMAT'S LAST THEOREM AND BEAL'S CONJECTURE OVER POLYNOMIAL AND FORMAL POWER SERIES RINGS

DANNY A. J. GÓMEZ-RAMÍREZ AND ALBERTO F. BOIX

ABSTRACT. In this paper, we study several Diophantine equations, like the one involved in Last Fermat's Theorem and Beal's equation, over the rings of polynomials and formal power series with coefficients on characteristic zero unique factorization domains. Moreover, we give general estimates of their number of polynomial solutions. Moreover, we study (non)extensions of Fermat's little theorem and the (non)existence of Wieferich primes over the univariate formal power series ring with real coefficients.

INTRODUCTION

If x, y, z are three strictly positive integers such that

$$x^n + y^n = z^n$$

for some integer strictly positive n, then $n \leqslant 2$. This is the statement of the so–called *Fermat's Last Theorem* (from now on, FLT for short) which, since its formulation in 1637 by Pierre de Fermat, influenced the research of a big portion of the mathematical community until Wiles and Taylor provided a full proof of it [21, 19]. One of the motivations of the present paper is given by the following:

Question 0.1. Let R be a unique factorization domain, and let u, v, w elements of R satisfying

$$u^n + v^n = w^n$$

for some positive integer n. Assume that u, v, w are relatively prime elements. Is it true that $n \leqslant 2$?

Of course, FLT says that the answer is yes provided $R = \mathbb{Z}$. When $R = \mathbb{R}[t]$, the result is also true as proved by Laeng in [10, Theorem 0.1]. Moreover, also in [10], it is claimed that the same statement holds when $R = \mathbb{R}[x_1, \ldots, x_n]$; however, the argument used there, invoking numerical substitution, is not

2020 *Mathematics Subject Classification.* Primary 11D41, 11D72. Secondary 13F25.

Key words and phrases. Fermat's Last Theorem for polynomial rings, Diophantine analysis, Beal's equation.

clear for us to hold, mainly because, among other issues, once we make numerical substitution, we have no guarantee to preserve the coprimality conditions among the solution tuple we start with.

The first goal of this paper is to show that FLT holds for any polynomial ring in several variables with coefficients on a unique factorization domain (from now on, UFD for short) of characteristic zero (see Theorem 1.10). Our approach is based on a generalization we provide of the so–called Stothers–Mason theorem[1] [11, Chapter IV, Theorem 7.1] for polynomial rings with coefficients on a UFD of characteristic zero (see Theorem 1.8) which follows so closely the approach developed in [16]. On the other hand, we also plan to show that, over certain formal power series ring, FLT does not hold, meaning that Fermat's equation admits infinitely many solutions.

Also motivated by FLT, the so–called *Tijdeman–Zagier's conjecture* [5, page 65] claims that the equation

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

has no solutions in integers $p, q, r \geqslant 3$ and relatively prime integers x, y, z. As announced in [13], the banker Andrew Beal offers 1 million dollars for the person who either prove it or can find a counterexample. Because of this reward, often this conjecture is known as *Beal's conjecture*.

Our interest again in this conjecture is concentrated in the following:

Question 0.2. Let R be a unique factorization domain, and let u, v, w elements of R satisfying

$$u^a + v^b = w^c$$

for some positive integers a, b, c. Assume that u, v, w are relatively prime elements. Is it true that all the exponents a, b, c are less or equal than 2?

Our second main result (see Proposition 2.1) is that, when R is a polynomial ring with coefficients on an integral domain, then the equation

$$u^a + v^b = w^c$$

has infinitely many polynomial solutions with arbitrarily large degree. Our approach is based on an argument given by Barghout in [2], where solutions of the equation are produced through a certain binomial substitution.

Another classical result is *Fermat's Little Theorem* [9, page 67, Theorem 4.3], which says that, for any integer x and for any prime number p,

$$x^{p-1} \equiv 1 \pmod{p}.$$

[1] In the literature, this theorem is usually called either Mason's theorem or Mason–Stothers' theorem. In this paper, we have adopted the terminology Stothers–Mason's theorem because, to the best of our knowledge, the first who proved the theorem was Stothers.

This statement was generalized by Euler in 1760 [9, page 86, Theorem 5.3], who proved that, for any positive integer m,

$$x^{\varphi(m)} \equiv 1 \pmod{m},$$

where $\varphi(m)$ is Euler's totient function which counts the number of integers between 0 and $m-1$ that are coprime with m. Both results, Fermat's Little Theorem and Euler's Theorem, have been generalized in [4] for certain rings (that are not necessarily commutative), the interested reader may like to consult [4, Theorems 3.5 and 3.7] for details. It is also well–known that both Fermat's Little Theorem and Euler's Theorem can be regarded as particular cases of Lagrange's Theorem, which says that the order of any element of a finite group divides the order of that group. Notice that Lagrange's Theorem is even known for some group schemes, the interested reader may like to consult [20] and the references given therein.

The final goal of this paper is to show that Fermat's Little Theorem is not true for the formal power series ring $\mathbb{R}[\![x]\!]$.

Now, we provide a more detailed overview of the contents of this paper for the convenience of the reader. In Section 1, we prove as main result (see Theorem 1.10) that FLT holds for any polynomial ring in several variables with coefficients in any UFD of characteristic zero. The key point in our proof of this statement is a generalization of Stothers–Mason's Theorem (see Theorem 1.8) which is interesting in its own right. Also in this section, we provide examples of commutative rings where FLT fails.

Secondly, in Section 2 we prove as main result (see Theorem 2.1) that we can produce infinitely many polynomial solutions to Beal's equation.

Finally, in Section 3 we show (see Theorem 3.3) that Fermat's little theorem does not hold over the formal power series ring $\mathbb{R}[\![x]\!]$.

1. Fermat's Last Theorem for Polynomial Rings in Several Variables over Suitable Commutative Rings

As explained along the Introduction, the goal of this section is to prove a polynomial version of Fermat's Last Theorem (FLT) for a broader collection of rings of coefficients including $\mathbb{Z}$, fields k of characteristic zero, and rings of polynomials in several variables with coefficients on these rings. More generally, our aim is to prove that FLT holds for the ring of polynomials $R[x]$, where R is a Unique Factorization Domain (UFD) of characteristic zero (i.e., no addition of $m-$times the unity of R is zero for all $m \in \mathbb{Z}_{\geqslant 1}$). We include implicitly fields of characteristic zero as UFD of characteristic zero, fulfilling trivially the factorization's condition. Our main methodological line is based on getting a suitable generalization of N. Snyder's elementary proof of Stothers–Mason's Theorem [16]. We also give the explicit proofs for the results in the polynomial ring in one variable for the sake of completeness in our presentation. However, this is a well-known result in the literature in the case where the

ring of coefficients is a field (see for instance [10]). On the other hand, the polynomial case with more than one variable and with a broader collection of coefficient rings is not explicitly known in the literature and needs an explicit and correct proof.

1.1. **Some preliminaries.** First, we need to state the following basic definitions.

Definition 1.1. Let R be a commutative ring with unity and $S = R[x]$. If $f(x) = \sum_{i=0}^{m} a_i x^i \in S$, we define the formal derivative of $f(x)$, denoted by $D(f)$ by the formula

$$D(f) = \sum_{i=0}^{m} i a_i x^{i-1},$$

where if $i \in \mathbb{N}$, then i can be seen as element of R via the multiplicative unity of R, i.e., $i \in R$ is simply the addition of $i-$times $1 \in R$. Moreover, the initial term of the former definition is understood as the formal derivative of a constant polynomial as is defined as zero, i.e., $D(a_0) = D(a_0 x^0) = 0.a_0 x^{0-1} = 0$.

It is a straightforward computation to verify that for all $f, g \in S$, $D(f+g) = D(f) + D(g)$, and $D(fg) = fD(g) + gD(f)$.

Let us recall the elementary fact that R is a UFD if and only if so is $R[x]$ (see, for example, [6, Corollary 8.2]). In particular, the notions of irreducible and prime coincides. Moreover, the factorization of an element in R or $R[x]$ is unique up to the order of the summands, and up to associates. In particular, there are infinitely many units in the ring of consideration if and only if each prime element has infinitely many associated elements.

Definition 1.2. Let R be a UFD and $S = R[x]$. Let $f, g \in S$. By simplicity in the notation assume that $p_1, \ldots, p_m \in S$ is the collection of primes dividing either f or g. Then, we can write the following expressions for the factorizations of them, $f = u \prod_{i=1}^{m} p_i^{a_i}$, and $g = v \prod_{i=1}^{m} p_i^{b_i}$, where some a_i, b_j can be zero, and u, v are units in S. Then, we define *a greatest common divisor of f and g*, denoted by $\gcd(f, g)$, as $\gcd(f, g) = \prod_{i=1}^{m} p_i^{\min(a_i, b_i)}$.

Before going further, we want to review the following classical notion in the study of polynomials.

Definition 1.3. Let $\mathbb{K}$ be a field, let $f \in \mathbb{K}[x_1, \ldots, x_n]$ be a non–constant polynomial, and write

$$f = \prod_{i=1}^{m} p_i^{\nu_i},$$

where $m \geqslant 1$, $\nu_i \geqslant 1$ and the polynomials p_i's are irreducible. Set

$$f_{\mathrm{red}} := \prod_{i=1}^{m} p_i,$$

which is called the *squarefree part (or the reduction) of* f.

Next result provides useful information about the squarefree part of a polynomial, we refer to [3, pages 186–187, Propositions 9 and 10] for details. Recall that, given a commutative ring B and given an ideal $J \subset B$, the radical of J is defined as

$$\sqrt{J} := \{b \in B \mid \ b^n \in J \text{ for some } n \in \mathbb{N}_0\}.$$

Proposition 1.4. *Let $\mathbb{K}$ be a field, let $f \in \mathbb{K}[x_1, \ldots, x_n]$ be a non–constant polynomial. Then, the following assertions hold.*

(i) We have $\sqrt{(f)} = (f_{\mathrm{red}})$. In other words, the squarefree part of f is nothing but a choice of a generator of the radical of the ideal generated by f.

(ii) If, in addition, $\mathbb{Q} \subseteq \mathbb{K}$, then we have

$$f_{\mathrm{red}} = \frac{f}{\gcd\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right)}.$$

In this way, in the next definition we extend the notion of the squarefree part of a polynomial to polynomial rings with coefficients in unique factorization domains. The definition looks as follows.

Definition 1.5. Let R be a UFD and $S = R[x]$, and let $f \in S$. Suppose that $f = u\prod_{i=1}^{n} p_i^{e_i}$, for some irreducible polynomials, $p_1, \ldots, p_n$, natural numbers $e_i \geqslant 1$, and some unit $u \in S$. Then, we define *a squarefree part of* f, denoted by f_{red}, as $f_{\mathrm{red}} = \prod_{i=1}^{n} p_i$.

Remark 1.6. Note that the notions of greatest common divisor and squarefree part are well-defined and are unique up to associates. In particular, in the context of $S = R[x]$, the degree of a greatest common divisor (gcd) and a squarefree part are well-defined, since the units of S are the units of R, so they are degree zero polynomials in S. Moreover, properties involving gcd-s and squarefree parts, like, for example, divisibility with other special elements of S are well-defined since these notions depends essentially on the unique factorization of S. In this sense we should understand the following statements where concepts like $\deg((f, g))$ appears. In other words, the reader can imagine any fixed gcd for following the deductions and computations. Additionally, to say that the gcd of a pair of numbers is 1 means, doing a little abuse in our notation, that the gcd is a unit, i.e., the corresponding numbers are coprime.

Next result can be regarded as a mild generalization of [3, page 187, Proposition 12].

Lemma 1.7. *Let R be a UFD and $S = R[x]$, and let $f \in S\backslash\{0\}$. Then,*

$$\left(\frac{f}{\gcd(f, D(f))}\right) \mid f_{\mathrm{red}}.$$

Proof. Firstly, if f is a unit, then our claim is trivial since all the elements involved in our divisibility relation are units. Secondly, let $f = u\prod_{i=1}^{n} p_i^{e_i}$, for different primes $p_1, \ldots, p_n$, natural numbers $e_i \geqslant 1$, and some unit $u \in S$. Then, $f_{\mathrm{red}} = \prod_{i=1}^{n} p_i$. So, for each i, we can write $f = p_i^{e_i} g_i$, where $\gcd(p_i, g_i) = 1$, for some $g_i \in S$. Thus, by the definition of formal derivative it holds

$$\begin{aligned} D(f) &= D(p_i^{e_i})g_i + p_i^{e_i} D(g_i) = e_i p_i^{e_i-1} D(p_i) g_i + p_i^{e_i} D(g_i) \\ &= p_i^{e_i-1}(e_i D(p_i) g_i + p_i D(g_i)). \end{aligned}$$

So, $\gcd(f, D(f)) = u\prod_{i=1}^{n} p_i^{d_i}$, where $e_i - 1 \leqslant d_i \leqslant e_i$, for all i. Thus, for each i, the power of p_i in the element $f/\gcd(f, D(f))$ is either zero or one. In conclusion, it means, by the definition of f_{red}, that $f/\gcd(f, D(f))$ divides f_{red}, as claimed. □

Now, we will prove a slightly more general version of Stothers–Mason's theorem [11, Chapter IV, Theorem 7.1], the key component of our subsequent extension of FLT. The interested reader on the original statements may like to consult [18] and [12, Corollary of page 156] for further information. The proof we present here is greatly inspired by [10, Proof of Mason's Lemma].

Theorem 1.8 (Generalization of Stothers–Mason's Theorem)**.** *Let R be a UFD and $S = R[x]$, and let $f, g, h \in S\backslash\{0\}$, be (pairwise) coprime elements such that $f + g = h$. Then, either $D(f) = D(g) = D(h) = 0$, or*

$$\max\{\deg(f), \deg(g), \deg(h)\} \leqslant \deg((fgh)_{\mathrm{red}}) - 1. \tag{1.1}$$

Proof. By assumption, we have the following identities:

$$\begin{cases} f + g = h \\ D(f) + D(g) = D(h). \end{cases}$$

Multiplying this system of equations by $D(g)$ and g respectively we obtain the system

$$\begin{cases} fD(g) + gD(g) = hD(g) \\ gD(f) + gD(g) = gD(h). \end{cases}$$

Now, starting from the top, subtracting the second equation to the first one we end up with the equality

$$fD(g) - gD(f) = hD(g) - gD(h).$$

From this equation, we deduce that the (pairwise) coprime elements $\gcd(f, D(f))$, $\gcd(g, D(g))$ and $\gcd(h, D(h))$ divides simultaneously $fD(g) - gD(f)$. So,

$$\gcd(f, D(f))\gcd(g, D(g))\gcd(h, D(h)) \mid (fD(g) - gD(f)). \tag{1.2}$$

Now, at this point and before doing a degree analysis, let us look ar the term $fD(g) - gD(f)$. Explicitly, assume for a moment that $fD(g) - gD(f) = 0$. Then, $f|D(f)$, $g|D(g)$ and, subsequently, $h|D(h)$, since $\gcd(f, g) = 1$, $\gcd(g, h) = 1$, respectively. Thus, it implies necessarily that $D(f) = D(g) = D(h) = 0$, which is the first possibility of our theorem.

So, assume that $fD(g) - gD(f) \neq 0$. So, we can genuinely say compare the degrees of the elements in (1.2). Then, using the degree inequalities from Lemma 1.7 and (1.2), and elementary degree estimates we get

$$\deg(f) + \deg(g) + \deg(h) - \deg(f_{\text{red}}) - \deg(g_{\text{red}})) - \deg(h_{\text{red}}) \leqslant$$
$$\leqslant \deg(f) + \deg(g) - 1.$$

Rearranging and using the coprimality of the three elements, we get

$$\deg(h) \leqslant \deg(f_{\text{red}}) + \deg(g_{\text{red}}) + \deg(h_{\text{red}}) - 1 = \deg((fgh)_{\text{red}}) - 1.$$

Finally, we can repeat exactly the former arguments with the equations $f = h + (-g)$ and $g = h + (-f)$, to obtain the last inequality replacing $\deg(h)$ by $\deg(f)$ and $\deg(g)$, respectively.

In conclusion, since the right-side term remains the same we obtain

$$\max\{\deg(f), \deg(g), \deg(h)\} \leqslant \deg((fgh)_{\text{red}}) - 1.$$

This finishes our proof. □

In our former setting, assume that there exists $f, g, h \in S$, and a natural exponent $n \geqslant 3$ such that $f^n + g^n = h^n$. Since our equation is homogeneous of degree n, we can factor out a greatest common divisor of f, g and h to obtain a new similar equation with a triple $f', g', h' \in S$ of (pairwise) coprime elements. So, if after factoring out the gcd we obtain genuine non-constant coprime polynomials, then we consider these type of genuine solutions. Even more, in our setting the collection of non-interesting or trivial solutions is a little bit broader that in the classic case of the integers. Explicitly, for us not only solutions when one of the polynomials vanishes, or the three polynomials are constants are trivial, but also solutions where the three polynomials are essentially the same (i.e. equal up to units) are trivial as well. For example, assume that $R = \mathbb{C}$, then we can construct a special collection of domain-specific non-interesting solutions of the form,

$$f^n + f^n = (\sqrt[n]{2}f)^n,$$

where f is any non-zero (non-constant) polynomial in $\mathbb{C}[x]$, $n \in \mathbb{Z}_{\geqslant 2}$, and $\sqrt[n]{2}$ can be any complex $n-$th root of 2. In conclusion, if there exist non-trivial interesting solutions of the Fermat equation, then coprime (non-constant) interesting solution must exist as well.

So, our next theorem states that in our former collection of coefficient rings there are only trivial solutions to Fermat's equation. The following statement can be regarded as the main result of this section.

Theorem 1.9 (FLT for Polynomial Rings in one variable over a UFD of Characteristic Zero)**.** *Let R be a UFD of characteristic zero and $S = R[x]$. Assume that there exist (pairwise) coprime polynomials $f, g, h \in S\backslash\{0\}$ and a natural number $n \geqslant 3$, such that*

$$f^n + g^n = h^n.$$

Then, f, g and h are constant polynomials.

Proof. Stothers–Mason's theorem 1.8 tells us that either $D(f) = D(g) = D(h) = 0$, which implies in our characteristic zero setting that $f, g, h \in R$, i.e., our elements are constant polynomials, as desired. So, to finish our proof is it enough to show that the second possible case of Stothers–Mason's theorem 1.8 leads to a contradiction, i.e.,

$$\max\{\deg(f^n), \deg(g^n), \deg(h^n)\} \leqslant \deg((f^n g^n h^n)_{\mathrm{red}}) - 1. \tag{1.3}$$

Effectively, in the following chain of inequalities we use the facts that, by definition, the squarefree part of an element coincides with the squarefree part of any power of it, and the fact that the maximum of a finite collection of numbers is always greater of equal than their average, and $n \geqslant 3$. Thus, we have

$$\begin{aligned}
&\deg(f) + \deg(g) + \deg(h) \leqslant (n/3)(\deg(f) + \deg(g) + \deg(h)) \\
&= (\deg(f^n) + \deg(g^n) + \deg(h^n))/3 \leqslant \max\{\deg(f^n), \deg(g^n), \deg(h^n)\} \\
&\leqslant \deg((f^n g^n h^n)_{\mathrm{red}}) - 1 = \deg((fgh)_{\mathrm{red}}) - 1 \\
&= \deg(f_{\mathrm{red}}) + \deg(g_{\mathrm{red}}) + \deg(h_{\mathrm{red}}) - 1 \leqslant \deg(f) + \deg(g) + \deg(h) - 1,
\end{aligned}$$

which is a contradiction. □

Theorem 1.10 (FLT for Polynomial Rings in several variables)**.** *Let R be a UFD of characteristic zero and $T = R[x_1, \ldots, x_m]$, with $m \geqslant 1$. Assume that there exist (pairwise) coprime polynomials $f, g, h \in T\backslash\{0\}$ and a natural number $n \geqslant 3$, such that*

$$f^n + g^n = h^n.$$

Then, f, g and h are constant polynomials.

Proof. Assume by the sake of contradiction that at least one of the polynomials is not constant, let's say $f \in T$ (the other cases are solved exactly in the same manner). After permutation of the variables we can assume that f is non-constant in the variable x_m. So, if $R' = R[x_1, \ldots, x_{m-1}]$, then $f \in R'[x_m]$ is not constant. Note that R' is again a UFD of characteristic zero. Moreover, since both $T \cong R'[x_m]$ possess the same factorization's structure, then f, g and h as elements of $R'[x_m]$ are (pairwise) coprime as well. Thus, by Theorem 1.9 f, g and h are constant polynomials of $R'[x_m]$, which is an absurd, since f is not a constant element of $R'[x_m]$. □

Remark 1.11. The proof of Theorem 1.10 is a natural and rigorous manner of generalizing FLT for polynomial rings in several variables. On the other hand, informal guidelines of doing such a generalization simply by *substitute numerical values for all the values, except one, and obtain one-variable solution that would contradict theorem 1.9* [10, pag. 2], are so straightforward and simple if one takes a closer look at it. In fact, this approach can be too informal and vague. Explicitly, when one evaluates some of the variables of a fictive non-trivial solution to Fermat's polynomial equation, one needs to guarantee that the resulting polynomials in one variable are non-zero elements, and pairwise coprime. Nonetheless, by evaluating one can immediately lose, on the one hand, the arithmetic relation between the original polynomials (e.g., being pairwise coprime), and, on the other hand, they can vanish formally. For instance, set $f = xy^3 - yx$ and $g = zx - 1$ in $R[x, y, z]$. Then, doing the replacements $y = z = 1$ we vanish f. And, doing formal replacements for other variables (as a natural alternative), like, for example, $y = x = z$ we would obtain $f = x^2(x^2 - 1)$ and $g = x^2 - 1$, which are not coprime. So, as far as the authors can see there is no elementary universal process of substitution preserving all the former properties from an hypothetical arbitrary counterexample of FLT in several variables.

Remark 1.12. The whole statement of theorem 1.10 is true even in the special case that FLT holds over the coefficient ring. However, the conclusion is not so useful in this case. So, let us rewrite a more explicit and enlightening form of theorem 1.10 taking into account this additional feature.

Definition 1.13. Let D be commutative ring with unity (or a UFD), then we say that *FLT holds in* D if for all natural number $n \geqslant 3$ there exist no triple $(a, b, c) \in D^3 \backslash \{(0, 0, 0)\}$ of (pairwise coprime) elements such that $a^n + b^n = c^n$.

Note that in the setting of UFD's we can omit the condition of coprimality in Definition 1.13 to obtain exactly the same notion. Explicitly, for any counterexample triple we could either multiply by or cancel out a common (non-invertible) factor in the corresponding Fermat's equation to obtain either a coprime or a non-coprime counterexample triple.

Theorem 1.14. *Let $\mathbb{D}$ be a UFD fulfilling FLT. Set $T = \mathbb{D}[x_1, \ldots, x_m]$, with $m \geqslant 1$. Then, FLT holds in the UFD T.*

Proof. It follows of Theorem 1.10, since a counterexample triple for FLT in T^3 would immediately lead to a counterexample triple for FLT in $\mathbb{D}^3$. □

1.2. **The Wide Nature of Counterexamples of Fermat's Last theorem for Several Collections of Commutative Rings with Unity.** Here, we study in some detail the nature of counterexamples of FLT for several kinds of commutative rings with unity and varying also the characteristic of the algebraic

structures in consideration. Let us start with a standard source of counterexamples for FLT.

Firstly, if we are considering a positive characteristic ($p > 0$) UFD D, then there are infinitely many exponents $n \in \mathbb{N}$, such that Fermat's equation has lots of non-trivial solutions. In fact, for exponents of the form p^m, for any $m \geqslant 1$, we have that for each pair of arbitrary polynomials $f, g \in D[x]$, the special arithmetic of D allows us to get equalities of the form

$$(f+g)^{p^m} = f^{p^m} + g^{p^m},$$

which provides a canonical source of solutions of Fermat's equation, or, equivalently, of counterexamples of FLT in this particular setting.

Secondly, a simple source of natural counterexamples, sometimes considered as 'trivial' (non-interesting) solutions of Fermat's equation is given when our commutative ring in consideration R contains an algebraically closed field F. In this case, for any $n \geqslant 2$ and any arbitrary $a, b \in F$, we can generate in a systematic manner infinitely many counterexamples to FLT in the following way

$$a^n + b^n = (\sqrt[n]{a^n + b^n})^n. \tag{1.4}$$

Note that (1.4) always has solutions due to the fact that F is algebraically closed.

Thirdly, a far more interesting source for counterexamples of FLT in characteristic zero emerges when we considered algebraic structures with an interesting arithmetic and, ideally, as similar as possible as the one of the integers.

A very natural candidate will be a structure of formal series over a coefficient ring very similar to $\mathbb{Z}$, but perhaps with some more units. So, it turns out that in this case we can find highly more interesting solutions to Fermat's equation as the following proposition will show.

Proposition 1.15. *Let $n \in \mathbb{N}_{\geqslant 1}$, let $\mathbb{Z}_{(n)}$ be the localization of $\mathbb{Z}$ in the multiplicative system form by the powers of n, and $R = \mathbb{Z}_{(n)}[\![x]\!]$. Then, there are (uncountable) infinitely many (non-trivial) non-constant and non-invertible solutions to Fermat's equation*

$$a^n + b^n = c^n, \tag{1.5}$$

for $a, b, c \in R$.

Proof. First of all, let us review some basic properties about the arithmetic of R.

Let us use the following generic notation for elements of R: $h = \sum_{i=1}^{\infty} h_i x^i$.

From the multinomial theorem [17, page 28] we have

$$\left(\sum_{i=0}^{m} x_i\right)^n = \sum_{\substack{k_0,\ldots,k_m\in\mathbb{N}\\ 0\leqslant k_j\leqslant n\\ \sum_{j=0}^{m} k_j=n}} \binom{n}{k_0,\ldots,k_m} \prod_{j=0}^{m} x_j^{k_j}.$$

From here, we obtain the corresponding extended formula with infinitely many summands inside the exponent

$$\left(\sum_{i\geqslant 0} x_i\right)^m = \sum_{\substack{\{k_j\}_{j\in\mathbb{N}}\\ 0\leqslant k_j\leqslant n\\ \sum_{j=0}^{\infty} k_j=n}} \binom{n}{\{k_j\}_{j\in\mathbb{N}}} \prod_{j=0}^{\infty} x_j^{k_j},$$

where due to the conditions of the $\{k_j\}_{j\in\mathbb{N}}$, only a finite number of them are different from zero.

Subsequently, applying the former formula in our context of formal power series, we obtain, as in [7, page 763],

$$h^n = \left(\sum_{i\geqslant 0} h_i x^i\right)^n = \sum_{i\geqslant 0} h_i^{(n)} x^i,$$

where

$$h_i^{(n)} = \sum_{\substack{\{k_j\}_{j\in\mathbb{N}}\\ 0\leqslant k_j\leqslant n\\ \sum_{j=0}^{i} k_j=n\\ \sum_{j=1}^{i} jk_j=i}} \binom{n}{k_0,\ldots,k_i} \left(\prod_{j=0}^{i} h_j^{k_j}\right).$$

Let us determine the largest $j\in\mathbb{N}$ such that some power of h_j appears as summand of this coefficient. Clearly, the largest $j\in\mathbb{N}$ that can appear in the equation $g=\sum_{j=0}^{\infty} jk_j$, with the corresponding $k_j\neq 0$. is $j=g$. In fact, the only possible combination of k_j-s fulfilling $k_g\neq 0$ and $g=\sum_{j=0}^{\infty} jk_j$ is $k_0=n-1$ and $k_g=1$. So, the summand containing a factor h_j with the largest possible j and fixed degree g is $j=g$, and the corresponding summand is exactly $nh_0^{n-1}h_g$. Thus, all the other summands of the coefficient of x^g fulfill that the $k_j\neq 0$, satisfy simultaneously the condition $j<g$, and this implies that the corresponding h_j appearing as factor of it possess a j strictly smaller that g. So, we can rewrite this coefficient in the following manner

$$nh_0^{n-1}h_g + \sum_{\substack{\{k_j\}_{0\leqslant j\leqslant g-1}\\ 0\leqslant k_j\leqslant n\\ \sum_{j=0}^{g-1} k_j=n\\ \sum_{j=0}^{g-1} jk_j=g}} \binom{n}{k_0,\ldots,k_{g-1}} \left(\prod_{j=0}^{g-1} h_j^{k_j}\right).$$

Moreover, from the last discussion we can deduce as well that among the coefficients of the power of x in h^n, the first time that h_g appears is exactly as coefficient of x^g.

With these elementary preliminaries, let us prove our proposition by induction on $j \in \mathbb{N}$, solving recursively the coefficients a_j, b_j and c_j.

Effectively. let us start with the initial case $j = 0$. In this case, we need to solve the equation

$$a_0^n + b_0^n = c_0^n, \tag{1.6}$$

for $a_0, b_0, c_0 \in \mathbb{Z}_{(n)}$.

Translating the last equation in the context of $\mathbb{Z}$ and multiplying by a suitable power of n, being, in fact, a multiple of n, we can rewrite it as follows

$$(n^{e_1} a_0')^n + (n^{e_2} b_0')^n = (n^{e_3} c_0')^n, \tag{1.7}$$

for some $e_1, e_2, e_3, a_0', b_0'.c_0' \in \mathbb{N}$. On the other hand, (1.7) has non-trivial solution only when $n = 2$, see for instance [14].

For $n = 3$, Fermat's Last Theorem says that (1.7) has only trivial solution with at least one of the summands equal to zero, which implies that either a_0, b_0 or c_0 equals zero. Then, let us assume, by simplicity, that $b_0 = 0$. In this case, let us choose an arbitrary unit of $\mathbb{Z}_{(n)}$ as the value of a_0 and c_0 (even for the case $n = 2$). In this manner we find suitable elements for the coefficient of x^0 in Fermat's equation.

Let us assume by a complete induction's hypothesis that all the coefficients $a_j, b_j, c_j \in \mathbb{Z}_{(n)}$, fulfilling the corresponding equations of coefficients of x^j Fermat's equation for all $j < g$.

So, let us determine $a_g, b_g, c_g \in \mathbb{Z}_{(n)}$.

Using the generic coefficient's formula of x^g discussed before we see that Fermat's equation for the coefficients of x^g gives the equation

$$nc_0^{n-1}c_g + \sum_{\substack{\{k_j\}_{0\leqslant j\leqslant g-1} \\ 0\leqslant k_j\leqslant n \\ \sum_{j=0}^{g-1} k_j = n \\ \sum_{j=0}^{g-1} jk_j = g}} \binom{n}{k_0, \ldots, k_{g-1}} (\prod_{j=0}^{g-1} c_j^{k_j}) =$$

$$na_0^{n-1}a_g + \sum_{\substack{\{k_j\}_{0\leqslant j\leqslant g-1} \\ 0\leqslant k_j\leqslant n \\ \sum_{j=0}^{g-1} k_j = n \\ \sum_{j=0}^{g-1} jk_j = g}} \binom{n}{k_0, \ldots, k_{g-1}} (\prod_{j=0}^{g-1} a_j^{k_j}) +$$

$$nb_0^{n-1}b_g + \sum_{\substack{\{k_j\}_{0\leqslant j\leqslant g-1}\\ 0\leqslant k_j\leqslant n\\ \sum_{j=0}^{g-1}k_j=n\\ \sum_{j=0}^{g-1}jk_j=g}} \binom{n}{k_0,\ldots,k_{g-1}} (\prod_{j=0}^{g-1} b_j^{k_j}).$$

Thus, since exactly in this equation appears for the first time the coefficients a_g, b_g and c_g and $c_0 \neq 0$, we can choose arbitrary values for a_g and b_g in $\mathbb{Z}_{(n)}$, and since nc_0^{n-1} is a unit in $\mathbb{Z}_{(n)}$, we can solve the last equation for c_g in a suitable manner in $\mathbb{Z}_{(n)}$.

So, by induction, we can find suitable coefficients for a, b and c such that they fulfill (1.5). Finally, due to the freedom in the countable infinitely many coefficients of a and b for $j > 0$, we can generate (uncountable) many solutions of Fermat's equation in R. Note, that since $b_0 = 0$, b is not a unit of R. In conclusion, we can generate (uncountable) infinitely non-trivial solutions with one of the summands non-invertible, and multiplying each of such solutions by x^n, we obtain uncountable many non-invertible non-constant solutions. □

As an immediate consequence we have the following theorem obtaining uncountable many solutions to Fermat's equation for all $n \in \mathbb{N}_{\geqslant 1}$ in a global coefficient containing all the possible inverses of the (fixed) powers of the equation.

Theorem 1.16. *Let $D = \mathbb{Q}[\![x]\!]$. Then, for all $n \in \mathbb{N}$ there are (uncountable) infinitely many (non-trivial) non-constant solutions to Fermat's equation*

$$a^n + b^n = c^n, \tag{1.8}$$

for $a, b, c \in D$, where at least one (or all) the terms $a, b,$ and c is not a unit in D.

Proof. This is an immediate consequence of Proposition 1.15, since $\mathbb{Q}$ contains all the localizations $\mathbb{Z}_{(n)}$, and therefore all the (uncountable many) solutions given in Proposition 1.15 lie as well in D, and the corresponding summands without independent terms remain also non-invertible in D. □

Remark 1.17. As the reader can easily see, Theorem 1.16 provides uncountable many non-trivial non-constant non-invertible solutions to Fermat's equation in a formal power series ring of characteristic zero.

Following the guidelines of the proof of Proposition 1.15, we can prove immediately the next more general result.

Proposition 1.18. *Let $n \in \mathbb{N}$, let D be a commutative ring with unity such that $n1_D \in D$ is a unit (notice that this condition is equivalent to say that $\mathbb{Z}_{(n)} \subseteq D$),*

and set $R = D[\![x]\!]$. Then, there are (uncountable) infinitely many (non-trivial) non-constant and non-invertible solutions to Fermat's equation

$$a^n + b^n = c^n, \tag{1.9}$$

for $a, b, c \in R$.

2. Beal's Equation and Related Diophantine equations in Polynomial Rings over an Integral Domain

In this section, we study the famous Beal's equation in the context of ring of polynomials (or formal power series) in several variables over an integral domain R. Beal's equation appears in the context of Beal–Tijdeman–Zagier's conjecture, which generalizes Fermat's Last Theorem, i.e., the equation

$$A^x + B^y = C^z \tag{2.1}$$

with positive integers A, B, C, x, y, z and $x, y, z > 2$ can only be fulfilled if $\gcd(A, B, C) > 1$ (see either [13] or [5, page 65]). It remains still an open conjecture and there is a reward of 1 million dollars for the person who either prove it or can find a counterexample.

The goal of this section is to study (2.1) regarding initial estimates of its number of solutions over $R[x_1, \ldots, x_n]$ as well as $R[\![x_1, \ldots, x_n]\!]$. For the sake of simplicity let us unify notation as follows. By $R(\!|\mathbf{x}|\!)$ we will always denote either $R[x_1, \ldots, x_n]$ or $R[\![x_1, \ldots, x_n]\!]$, in a consistent manner clear from the context. We simply do this because some results below will be true in both situations and the proofs of both cases will be methodological copies of one another. Note that, although the arithmetic of $R[x_1, \ldots, x_n]$ and $R[\![x_1, \ldots, x_n]\!]$ are qualitatively different, sometimes it is useful to see $R[x_1, \ldots, x_n]$ contained in $R[\![x_1, \ldots, x_n]\!]$, as we shall see in the next results. For the definition of a monomial ordering on a polynomial ring, the reader is referred to [8, page 10, Definition 2.1]. Moreover, in the next proposition we write $\mathbf{x} = (x_1, \ldots, x_n)$.

Proposition 2.1. *Let R be an integral domain, $W := R[\mathbf{x}]$, and $T := R[\![\mathbf{x}]\!]$. So, $W \subseteq T$. Then, the exponential Diophantine equation*

$$A^d + B^e = C^f, \tag{2.2}$$

where $A, B, C \in R(\!|\mathbf{x}|\!)$, and $d, e, f \in \mathbb{N}$ with $d, e, f > 2$; has infinitely many solutions for arbitrarily large d, e, f. Moreover, the following statements hold.

- *(i) Fixing a global monomial ordering, there are polynomials A, B, C of arbitrarily large degree that satisfies* (2.2).
- *(ii) Fixing a local monomial ordering, there are formal power series A, B, C of arbitrarily large order that satisfies* (2.2).

Proof. We take initial inspiration from the work by Kamal Barghout [2]. However, we present our calculations in a more compact and direct manner. Let

U, X, Y be symbolic variables ranging over elements in T, and $l, n \in \mathbb{N}$. Then, it is a straightforward to verify that

$$((U^l + Y^l)X^l)^n = (UX)^{nl} + ((U^l + Y^l)^n - U^{nl})X^{nl}. \tag{2.3}$$

Notice that (2.3) can be regarded as an element of $T[X, Y, U]$. Now, we consider the following T–algebra homomorphism:

$$T[X, Y, U] \longrightarrow T[Y, U]$$
$$X \longmapsto (U^l + Y^l)^n - U^{nl},\ Y \longmapsto Y,\ U \longmapsto U.$$

Now, setting $X := (U^l + Y^l)^n - U^{nl}$, and substituting in (2.3), we obtain

$$((U^l+Y^l)((U^l+Y^l)^n-U^{nl})^l)^n = (U((U^l+Y^l)^n-U^{nl}))^{nl}+((U^l+Y^l)^n-U^{nl})^{nl+1}. \tag{2.4}$$

Note that, in (2.4), on the one hand we can replace U and Y by any element of W and, on the other hand, we can replace l and n by any natural number and it remains true, since R (subsequently T) is a commutative ring with unity.

So, fixing a monomial order in the variables $x_1, \ldots, x_n$, it is straightforward to verify that for any arbitrarily large choice of $l, n \in \mathbb{N}$, we can choose polynomials $u, y \in W$ of arbitrarily large degree such that the three polynomial terms of (2.4) have arbitrarily large degrees, e.g., choosing $y \in W$ with an arbitrarily large and relatively bigger degree than the one of u.

On the other hand, notice that (2.4) can be regarded as a particular form of (2.2), with the following choices:

$$A := (U^l + Y^l)((U^l + Y^l)^n - U^{nl})^l,\ B := (-1)^{nl}U((U^l + Y^l)^n - U^{nl}),$$
$$C := (U^l + Y^l)^n - U^{nl},\ d := n,\ e := nl,\ f := nl + 1.$$

In conclusion, since we have enough freedom for the choices of l and n, and for the triples $(d = n, e = nl, f = nl + 1)$ to be arbitrarily large, and (2.4) is a particular form of (2.2), we see that (2.2) has infinitely many solutions for arbitrarily large d, e, f and with polynomials $A, B, C \in R(\!(\mathbf{x})\!)$ of arbitrarily large degree. □

We plan now to exhibit an explicit example of the construction used along the proof of Proposition 2.1, the unjustified calculations were carried out with Macaulay2.

Example 2.2. Following the notation used in Proposition 2.1, here $R = \mathbb{Q}$ and $W = R[x, y]$. Choosing $U = x$ and $Y = y$, we have, setting $n := 2$ and $l := 3$, that

$$A := 8x^{12}y^9 + 20x^9y^{12} + 18x^6y^{15} + 7x^3y^{18} + y^{21},\ B := 2x^4y^3 + xy^6,$$
$$C := 2x^3y^3 + y^6$$

is a solution of the equation $A^2 = B^6 + C^7$. Notice that, in this particular example, A, B and C are homogeneous polynomials of total degree 21, 7 and 6 respectively. On the other hand, it is also clear that polynomials A, B and C are far from being irreducible. Indeed, we have that

$$V(A) = V(y) \cup V(x+y) \cup V(x^2 - xy + y^2) \cup V(2x^3 + y^3),$$
$$V(B) = V(x) \cup V(y) \cup V(2x^3 + y^3),\ V(C) = V(y) \cup V(2x^3 + y^3),$$

where as usual, given $w \in W$, $V(w)$ denotes the Zariski closed set given by the prime ideals of W containing w. Finally, notice that the kernel of the $\mathbb{Q}$–algebra map

$$\mathbb{Q}[X, Y, U] \longrightarrow \mathbb{Q}[Y, U]$$
$$X \longmapsto (U^l + Y^l)^n - U^{nl},\ Y \longmapsto Y,\ U \longmapsto U.$$

is the ideal generated by $Y^6 + 2Y^3U^3 - X$.

Let us focus now on the formal power series case. In this case, choosing

$$U = \frac{x}{1-x},\ Y = \frac{y}{1-y},$$

we obtain formal power series $A,\ B,\ C$ (that of course can also be regarded as rational functions, that is, elements of $\mathbb{Q}[x, y]_{(x,y)}$) with the following properties:

(i) A is a rational function whose numerator is a polynomial of total degree 33.

(ii) B is a rational function whose numerator is precisely

$$-3x^4y^6 + 6x^4y^5 + 3x^3y^6 - 6x^4y^4 - 3x^2y^6 + 2x^4y^3 + xy^6.$$

In this way, B can be regarded as formal power series with total order at least 7 because of the term xy^6 appearing in the support of its numerator.

(iii) C is a rational function whose numerator is precisely

$$3x^3y^6 - 6x^3y^5 - 3x^2y^6 + 6x^3y^4 + 3xy^6 - 2x^3y^3 - y^6.$$

In this way, C can be regarded as formal power series with total order at least 6 because of the term y^6 appearing in the support of its numerator.

An special corollary of the proof of Proposition 2.1 will be a rough estimate of the cardinality of the polynomial solutions of the polynomial equation $A^n - B^n = C^{n+1}$, which describes when the differences of polynomials $n-$powers can give $(n+1)-$powers. For more information about this example the reader may consult our simple code in Macaulay 2.[2]

[2]https://github.com/DAJGomezRamirez/BealsAlgorithm/blob/main/ExampleOfBealsConstruction

Proposition 2.3. *Let R be an integral domain. Then, the exponential Diophantine equation*

$$A^n - B^n = C^{n+1}, \tag{2.5}$$

where $A, B, C \in R(\!(\mathbf{x})\!)$, and $n \in \mathbb{N}$ with $n > 0$; has infinitely many solutions for each n and with polynomials $A, B, C \in R(\!(\mathbf{x})\!)$ of arbitrarily large degree (fixing a monomial order).

Proof. Setting $l = 1$ in (2.4) and rearranging we obtain

$$((U+Y)((U+Y)^n - U^n))^n - (U((U+Y)^n - U^n))^n = ((U+Y)^n - U^n)^{n+1}. \tag{2.6}$$

In conclusion, since (2.6) is an special flexible form of (2.5), we can verify directly, as in the proof of Proposition 2.1, that (2.5) has infinitely many solutions for each n and with polynomials $A, B, C \in R(\!(\mathbf{x})\!)$ of arbitrarily large degree. □

3. Fermat's Little (Non)Theorem and Wieferich's Conjecture for the Ring of Formal Power Series over the Real Numbers

Motivated by [4, Theorem 3.5], where a generalization of Fermat's Little Theorem is proved for certain rings, the goal of this section is to explore the (non-)validity of Fermat's little theorem [9, page 67, Theorem 4.3] in a very natural setting where we can obtain a natural generalization for the notion of exponential function at least for constant series. Even more, inspired by the elementary theory of power series with real coefficients [15], a natural ring to define partially the exponential function is the ring of formal power series in one variable over the reals $\mathbb{R}[\![x]\!]$.

Definition 3.1. Let $S = \mathbb{R}[\![x]\!]$ and fix $a \in S$. Then, we formally define the exponentiation of a to x (or any polynomial in x) as follows.

$$a^x := \sum_{n \geqslant 0} \frac{(\ln a)^n}{n!} x^n.$$

One can straightforwardly verify that all the standard properties of formal exponents are immediately derived from the classic power series versions.

With the former definition in mind let us review the (non)plausibility of Fermat's little theorem:

Question 3.2. For any prime (formal power series) $p \in \mathbb{R}[\![x]\!]$ and any (real) element $a \in \mathbb{R}$, is it true that $a^{p-1} \equiv 1 \pmod{p}$?

Next statement is the main result of this section.

Theorem 3.3. *Fermat's little theorem does not hold in $\mathbb{R}[\![x]\!]$.*

Proof. First of all, we note that since $\mathbb{R}[\![x]\!]$ is a discrete valuation ring with essentially (up to units) a unique prime element x, generating the only maximal ideal. So, our question needs to be answered only in this case. Now, by definition we have

$$2^{x-1} = k_0 + k_1 x + k_2 x^2 + \dots,$$

for some real coefficients k_i, with $i \in \mathbb{N}$, and

$$k_0 = \sum_{m \geqslant 0} (-1)^m \frac{(\ln 2)^m}{m!} = 2^{-1} = \frac{1}{2}.$$

Thus, $2^{x-1} - 1 = -\frac{1}{2} + c_1 x + c_2 x^2 + \cdots$ is a unit in $\mathbb{R}[\![x]\!]$. Then, $2^{x-1} \not\equiv 1 \pmod{x}$, which implies that $2^x \not\equiv 2 \pmod{x}$. □

Remark 3.4. The fact that $2^x \not\equiv 2 \pmod{x}$ also implies that in $\mathbb{R}[\![x]\!]$ there are no Wieferich primes at all. Remember that an odd prime number is a Wieferich prime p if it fulfills a slightly stronger condition than the one involved in Fermat's little theorem, i.e., $2^{p-1} \equiv 1 \pmod{p^2}$. The interested reader on Wieferich primes may like to consult [1] and the references given therein for additional information.

ACKNOWLEDGEMENTS

Alberto F. Boix received partial support by grant PID2022-137283NB-C22 funded by MICIU/AEI/10.13039/501100011033. Danny A. J. Gomez-Ramirez sincerely thanks Jose Manuel Escorcia, Gabriel Loaiza , Cristhian Montoya and Luz Elena Giraldo for the support and kindness.

REFERENCES

1. W. D. Banks, F. Luca, and I. E. Shparlinski, *Estimates for Wieferich numbers*, Ramanujan J. **14** (2007), no. 3, 361–378. MR 2357442
2. K. Barghout, *Finding polynomial solutions to Beal's conjecture by expanding powers of binomials*, Available at `http://dx.doi.org/10.13140/RG.2.2.28727.88482`.
3. D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, fourth ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR 3330490
4. F. D. de Melo Hernández, C. A. Hernández Melo, and H. Tapia-Recillas, *Fermat's little theorem and Euler's theorem in a class of rings*, Comm. Algebra **50** (2022), no. 7, 3064–3078. MR 4420333
5. N. D. Elkies, *The ABC's of number theory*, The Harvard College Mathematics Review **1** (2007), no. 1, 57–76.
6. R. M. Fossum, *The divisor class group of a Krull domain*, Band 74, [Results in Mathematics and Related Areas], Springer-Verlag, New York-Heidelberg, 1973. MR 382254
7. X.-X. Gan and N. Knox, *On composition of formal power series*, Int. J. Math. Math. Sci. **30** (2002), no. 12, 761–770. MR 1917671
8. G.-M. Greuel and G. Pfister, *A **Singular** introduction to commutative algebra*, extended ed., Springer, Berlin, 2008, With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh and UNIX). MR 2363237

9. G. A. Jones and J. M. Jones, *Elementary number theory*, Springer Undergraduate Mathematics Series, Springer-Verlag London, Ltd., London, 1998. MR 1610533
10. E. Laeng, *Fermat's last theorem for polynomials*, Parabola **35** (1999), no. 1, 3–7.
11. S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556
12. R. C. Mason, *Equations over function fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 149–157. MR 756091
13. R. D. Mauldin, *A generalization of Fermat's last theorem: the Beal conjecture and prize problem*, Notices Amer. Math. Soc. **44** (1997), no. 11, 1436–1437. MR 1488570
14. A. Overmars, L. Ntogramatzidis, and S. Venkatraman, *A new approach to generate all Pythagorean triples*, AIMS Math. **4** (2019), no. 2, 242–253. MR 4135085
15. J. M. Ruiz, *The basic theory of power series*, Advanced Lectures in Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1993. MR 1234937
16. N. Snyder, *An alternate proof of Mason's theorem*, Elem. Math. **55** (2000), no. 3, 93–94. MR 1781918
17. R. P. Stanley, *Enumerative combinatorics. Volume 1*, second ed., Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012. MR 2868112
18. W. W. Stothers, *Polynomial identities and Hauptmoduln*, Quart. J. Math. Oxford Ser. (2) **32** (1981), no. 127, 349–370. MR 625647
19. R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR 1333036
20. E. Torti, *Lagrange's theorem for a family of finite flat group schemes over local Artin rings*, Available at `https://arxiv.org/pdf/2411.12129`.
21. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR 1333035

VISIÓN REAL COGNITIVA (COGNIVISIÓN) S.A.S. ITAGUÍ, COLOMBIA.
Email address: `daj.gomezramirez@gmail.com`

DEPARTMENT OF MATHEMATICS, UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH, AV. EDUARD MARISTANY 16, 08019, BARCELONA, SPAIN.
Email address: `alberto.fernandez.boix@upc.edu`