Último Teorema de Fermat: a história da equação $x^n + y^n = z^n$

Caio H. S. de Souza*

Universidade Federal de São Carlos

caiohsouza36@gmail.com

Resumo

Apresentaremos um dos maiores problemas da história da Matemática: o Último Teorema de Fermat. Aqui vamos contar sua origem, discutir dois casos particulares e ver alguns dos grandes nomes da comunidade matemática que ao longo dos séculos trabalharam com esta simples equação.

1. Introdução

Um dos campos da Matemática com problemas que desafiam os grandes matemáticos de todas as épocas e que contribuem para o crescimento desta ciência é sem dúvidas a Teoria dos Números. Grandes enigmas surgiram do estudos dos números inteiros e perduraram por muito tempo, alguns até hoje indecifrados. Seus teoremas quase sempre tem objetivos que aparentam ser muito simples, mas não podemos nos deixar enganar pelos enunciados: estes que podem parecer, para um desavisado, exercícios bobos acabam se revelando grandes problemas que necessitam às vezes de conexões inimagináveis entre áreas da Matemática para serem resolvidos. Um exemplo maravilhoso (e que este texto será sim capaz de conter) é o famoso problema proposto por Pierre de Fermat sobre as soluções de uma equação, que só recebeu uma resposta definitiva mais de 350 anos depois de Fermat!

Os pré-requisitos necessários ao leitor são os conceitos elementares de Teoria dos Números (divisão, máximo divisor comum, números primos e congruências), o Teorema Fundamental da Aritmética e certa familiaridade com números complexos.

2. A origem

Pierre de Fermat (1601 - 1665) foi um magistrado francês que atuava em Toulouse e tinha a Matemática como passatempo. Tal "hobby" o tornou famoso em sua época: foi um dos primeiros a desenvolver a Geometria Analítica e deu os primeiros passos em direção ao Cálculo. Mas, sua paixão era sem dúvidas a Teoria dos Números. Fermat trocava correspondência com grandes matemáticos de sua época, desafiando-os com problemas envolvedo suas descobertas sobre inteiros que, como todos os seus resultados, nunca foram publicados formalmente. De fato, segundo Edwards (1977, p.1), ele não tinha interesse em publicações e o que temos hoje contendo os teoremas de sua autoria é a coletânea de cartas e anotações publicadas postumamente por seu filho Samuel de Fermat.

Porém, falar de teoremas provados por Fermat é um tanto difícil. Muitos deles eram de fato conjecturas, pois ele não apresentava aos outros as demonstrações de muitas das suas

*Agradecimentos a Prof. Dra. Marina Andretta pelo convite e ao Prof Dr. Humberto Luiz Talpo, meu orientador, por apoiar minhas ideias

afirmações. Uma fonte destas conjecturas eram as margens do livro *Aritmética* (250 d.C.) de Diofanto de Alexandria, matemático grego responsável por um compilado (em 13 livros) de problemas envolvendo equações de segundo e terceiro grau e suas soluções racionais (e, quando restringimos as solução aos números inteiros, temos o que hoje chamamos **equações diofantinas**). No segundo livro da obra, o problema número 8 pede para "dado um número que é um quadrado, escrevê-lo como a soma de dois outros quadrados". Sobre este problema, Fermat faz uma anotação no livro que é o ponto de partida para um dos maiores enigmas da Matemática. Originalmente em latim e traduzida aqui do inglês [[EDWARDS], 1977, p.2], a anotação diz:

> Em contrapartida, é impossível para um cubo ser escrito como uma soma de dois cubos ou uma quarta potência ser escrita como uma soma de duas quartas potências ou, em geral, para qualquer número que é uma potência maior que a segunda ser escrito como uma soma de duas potências do mesmo tipo. Eu tenho uma demonstração maravilhosa desta proposição que esta margem é estreita demais para conter.

Temos então a equação $x^n + y^n = z^n$. Claramente $(0,0,0)$ é uma solução, bem como outras triplas contendo 0 como $(0, y, y)$. Porém, segundo Edwards (1977, p.3), na época o zero ainda era um conceito obscuro e Fermat se referia então apenas aos inteiros não nulos, excluindo a solução $(0,0,0)$ e a chance de algum dos termos ser nulo, estas chamadas soluções triviais. Não é claro também se a tripla (x, y, z) é composta por racionais ou inteiros, mas isso não é problema, pois uma solução racional (x, y e z racionais) implicaria uma solução inteira (x, y e z inteiros), bastando mutilpicar a equação pelo máximo divisor comum destes. Podemos ainda retirar os fatores comuns de x e y: se $d = mdc(x, y)$, fatorando-o ficamos com

$$x^n + y^n = z^n \Rightarrow (dx_0)^n + (dy_0)^n = z^n \Rightarrow d^n(x_0^n + y_0^n) = z^n \Rightarrow d^n | z^n \Rightarrow d | z.$$

A última implicação vem da aplicação do Teorema Fundamental da Aritmética[1]. Assim $z = dz_0$ e $x_0^n + y_0^n = z_0^n$, donde temos uma nova tripla com $mdc(x_0, y_0) = 1$ e, fazendo uma verificação rápida, $mdc(x_0, z_0) = mdc(y_0, z_0) = 1$. Esta solução (x_0, y_0, z_0) é uma solução primitiva do problema. Então, focamos na equação diofantina $x^n + y^n = z^n$ que recebe o nome de **equação de Fermat**. Declaramos desta forma a afirmação de Fermat como:

Para $n \geq 3$, a equação $x^n + y^n = z^n$ não possui soluções (primitivas) inteiras não triviais.

Samuel lançou uma nova edição de *Aritmética* contendo as anotações de Fermat no apêndice. Com isso, várias das conjecturas de Fermat se tornaram públicas e os matemáticos posteriores se empenharam em demonstrá-las e obtiveram sucesso em todas, exceto a afirmação que destacamos, que levou mais tempo para ser provada. Esta então fica conhecida como **Último Teorema de Fermat**.

3. O caso $n = 4$

O caso $n = 4$ pode ser deduzido através de uma técnica cujo primeiro registro de sua utilização está também em uma das margens da cópia que Fermat tinha de *Aritmética*, sendo então a ele atribuída a sua invenção. Estamos falando do método da **descida infinita**, que pode ser enunciado em termos lógicos da seguinte maneira:

[1] Para recordarmos, tal teorema afirma que todo número inteiro $n \notin \{-1, 0, 1\}$ ou é primo ou se escreve como produto de primos, sendo essa fatoração única a menos de ordem fatores

3.1. ***Princípio da Descida Infinita***: *Seja $P(n)$, $n \in \mathbb{N}$, uma propriedade qualquer do número natural n. Suponhamos que*

1. *P(0) é verdadeiro;*
2. *Para todo $k \in \mathbb{N}$, se $P(k)$ é falso então existe um número natural m tal que $m < k$ e $P(m)$ é também falso.*

Nessas condições, a propriedade $P(n)$ é válida para todo número natural n.

Inicialmente, o príncipio da descida infinita pode não parecer natural, mas podemos reescrevê-lo com um enunciado equivalente:

3.2. ***Princípio da Descida Infinita***: *Não existe sequência infinita estritamente decrescente no conjunto dos números naturais.*

Em [[KNEŽEVIC; KRTINIĆ], 2013, p.69] temos uma demonstração desta equivalência e como relacionam-se o Princípio de Indução Finita (fraco e forte), o Princípio da Boa Ordem e a descida infinita, mostrando que estes são de fato todos equivalentes.

Resolve-se o caso $n = 4$ utilizando o princípio acima aliado as ternas pitagóricas. Euclides, em *Os Elementos*, Livro X, exibe a forma geral das soluções inteiras positivas de $x^2 + y^2 = z^2$. Tomando uma solução primitiva (x, y e z dois a dois primos entre si), esta será determinada por

$$\begin{aligned} x &= r^2 - s^2 \\ y &= 2rs \\ z &= r^2 + s^2 \end{aligned}$$

para $r, s \in \mathbb{N}$ com $r > s$. Se r e s são primos entre si, a tripla pitagórica é dita primitiva. Podemos sempre tomar r e s com $mdc(r,s) = 1$ pois caso $r = d\bar{r}$ e $s = d\bar{s}$, teremos que $x = (\bar{r}^2 - \bar{s}^2)d^2$, $y = 2\bar{r}\bar{s}d^2$ e $z = (\bar{r}^2 + \bar{s}^2)d^2$, donde é fácil ver que $\bar{r}$ e $\bar{s}$ darão também origem a uma tripla pitagórica sem o fator d.

Teorema 3.3. *A equação $x^4 + y^4 = z^4$ não possui soluções inteiras não triviais.*

Demonstração: Seja (x, y, z) uma solução primitiva da equação de Fermat, com x, y e z positivos (a potência par nos permite isso). Em particular, $(x^2)^2 + (y^2)^2 = (\bar{z})^2$, ou seja, temos uma tripla pitagórica (com $\bar{z} = z^2$). Como $mdc(x,y) = 1 \Rightarrow mdc(x^2, y^2) = 1$, tais x^2, y^2 e z^2 são dois a dois primos entre si e então são determinados por

$$\begin{aligned} x^2 &= r^2 - s^2 \\ y^2 &= 2rs \\ \bar{z} &= r^2 + s^2 \end{aligned}$$

com $r > s > 0$, em particular $r > 1$. Vemos que $mdc(r,s) = 1$ (pois caso contrário o mdc destes ao quadrado seria fator de x^2 e y^2). Olhando para a primeira equação $x^2 + s^2 = r^2$, temos outra tripla pitagórica e $mdc(x,s) = 1$, pois $mdc(r,s) = 1$, donde vemos que r, s e x são dois a dois primos entre si. Logo, existem $a, b \in \mathbb{N}$, com $a > b$ e $mdc(a,b) = 1$ (lembre que podemos tirar os fatores de a e b), tais que

$$\begin{aligned} x &= a^2 - b^2 \\ s &= 2ab \\ r &= a^2 + b^2 \end{aligned}$$

Então $y^2 = 2rs = 4ab(a^2 + b^2)$. Afirmamos que ab e $a^2 + b^2$ são primos entre si. Suponhamos p primo que divide ambos. Como $mdc(a, b) = 1$, podemos tomar sem perda de generalidade $p|a$ e $p \nmid b$, o que implica $p|a^2$ e $p \nmid b^2$. Assim $a^2 = k_1 p$ e $b^2 = k_2 p + l$, com $0 < l < p$. Com isso $a^2 + b^2 = p(k_1 + k_2) + l \Rightarrow p \nmid (a^2 + b^2)$, contradição. Portanto $mdc(ab, a^2 + b^2) = 1$. Dessa forma temos o produto de dois números primos entre si que se igualam a um quadrado. Então cada fator do produto é também um quadrado.

De fato, para que $fg = p^n = p_1^n \ldots p_s^n$, com cada p_j primo e f e g primos entre si, então

$$f = p_{f1}^n \cdots p_{fk}^n \text{ e } g = p_{g1}^n \cdots p_{g(s-k)}^n,$$

com $p_{fi}, p_{gj} \in \{p_1, \ldots, p_s\}$ e $p_{fi} \neq p_{gj}$, $1 \leq i \leq k$, $1 \leq j \leq s - k$ devido a forma única de representação garantida pelo Teorema Fundamental da Aritmética. Assim

$$ab = v^2 \text{ e } a^2 + b^2 = w^2 \Rightarrow a = t^2, b = u^2 \text{ e } a^2 + b^2 = w^2.$$

Portanto

$$t^4 + u^4 = a^2 + b^2 = w^2,$$

onde t e u são primos entre si, pois caso contrário teríamos um divisor comum de a e b. Mais que isso, $w^2 = a^2 + b^2 = r < r^2 < \bar{z}$. Podemos então aplicar todo o raciocício acima e conseguir uma sequência infinita de termos decrescentes, ou seja, uma descida infinita. Como tal sequência não pode existir, pelo Princípio da Descida Infinita, tal solução inicial adimitida não existe. Concluímos assim a prova.

■

A resolução do caso particular vista reduz o problema de forma significativa: se $n = 2^m$, $m \geq 2$, então n é múltiplo de 4 e assim $x^n + y^n = z^n \Rightarrow (x^k)^4 + (y^k)^4 = (z^k)^4$, donde concluímos que o Último Teorema de Fermat vale para $n = 2^m$ e $n = 4k$. Fazer tal fatoração de n nos permite ir direto ao ponto: se $n = pq$, p primo ímpar, então

$$x^n + y^n = z^n \Rightarrow (x^q)^p + (y^q)^p = (z^q)^p$$

ou seja, se a equação de Fermat não adimitir solução para o primo p, então não terá também solução para $n = pq$. Por isso, voltamos nossa atenção aos primos ímpares.

4. O caso $n = 3$

A resolução do caso $n = 3$ do Último Teorema de Fermat é historicamente atribuída a Euler, como pode ser visto segundo tomo de *Obras de Lagrange*[2](1868), onde este menciona Euler como responsável pela demonstração. Existem porém controvérsias quanto a essa atribuição, pois a prova dada continha um argumento falacioso, que discutiremos. Mas tal falha pode ser corrigida, não de forma trivial, através de métodos que o próprio Euler utilizou em outras demonstrações. Vamos pontuar os principais passos da prova e focar na inquietação trazida pelo tal argumento falho.

Euler utilizou a técnica da descida infinita de Fermat. Começando com o problema nas condições essenciais, isto é, x, y e z primos entre si dois a dois, suponhamos que $x^3 + y^3 = z^3$.

[2]Oeuvres de Lagrange, tradução do autor

Como estes são primos entre si, no máximo um deles pode ser par e no mínimo um deve ser par, portanto exatamente um deles é par. Tomemos z par e x, y ímpares (os outros casos são todos análogos). Então $x + y = 2p$ e $x - y = 2q$ e podemos escrever então x e y em função de p e q (que são primos entre si, de paridades opostas e ambos positivos), tranformando o lado direito da equação de Fermat em

$$2p(p^2 + 3q^2) = z^3$$

A prova então se separa em dois casos: ou $2p$ e $p^2 + 3q^2$ não são primos entre si (e nesse caso $3|p$) ou estes são primos entre si. Vamos olhar o caso em que $2p$ e $p^2 + 3q^2$ não são primos entre si. Temos que $p^2 + 3q^2$ é ímpar (lembrando das paridades opostas) e se $m|2p$ e $m|(p^2 + 3q^2)$ então $m|p$ e $m|(p^2 + 3q^2) \Rightarrow m|p$ e $m|3q^2$, ou seja, 3 é o único fator comum possível, logo $3|p$. Portanto

$$z^3 = 2p(p^2 + 3q^2) = 3^2 2s(3s^2 + q^2),$$

onde agora $3^2 2s$ e $3s^2 + q^2$ são primos entre si. Então estes são cubos. Para que $3s^2 + q^2$ seja cubo, Euler diz que isso só pode ocorrer se, para inteiros a e b,

$$q = a(a - 3b)(a + 3b) \text{ e } s = 3b(a - b)(a + b)$$

e esta é a única forma disso acontecer. Para quaisquer a e b inteiros primos entre si, se tomarmos q e s nas formas acima basta fazermos as contas para vermos que $3s^2 + q^2$ é cubo. Porém, Euler dizia que esta era condição necessária e suficiente, ou seja, existiriam sempre a e b que fariam de $3s^2 + q^2$ um cubo. Aqui temos nosso impasse: Euler afirma: "Quando, por exemplo, $x^2 + cy^2$ é um cubo, pode-se certamente concluir que ambos os seus fatores irracionais[3] $x + y\sqrt{-c}$ e $x - y\sqrt{-c}$, devem ser cubos, porque eles são primos entre si e x e y não tem divisor comum" [[EDWARDS], 1977, p.44] e baseia a condição necessária e suficiente apresentada para $3s^2 + q^2$ neste "fato".

Euler não prova tal afirmação. Para números inteiros tal fato é verdadeiro, como vimos na prova do caso $n = 4$, mas podemos generalizar tão imediatamente assim sua validade para números da forma $x + y\sqrt{-c}$? O fato é que Euler lidava com estes números como quem trabalhava com os elementos de $\mathbb{Z}$, utilizando por exemplo o Teorema Fundamental da Aritmética nesse contexto. Para $c = 3$ a afirmação é verdadeira, mas existem muitos valores de c onde tal afirmação é falsa. Ou seja a afirmação de Euler é verdadeira pelo menos para caso $c = 3$ que utilizamos aqui na demonstração, porém o argumento que ele usa para justificá-la é obscuro e parte de uma generalização feita sem o devido cuidado. Para justificar o caso específico $c = 3$ devidamente e nos ambitos da Teoria dos Números elementar pode-se utilizar fatos presentes no trabalho *Elementos de Álgebra* (1828) do próprio Euler, através de uma prova um tanto longa [[EDWARDS], 1977, p.52-54] e que se diferencia muito da que fizemos em $\mathbb{Z}$.

Concluíndo a demonstração, como $3^2 2s$ é um cubo, substituindo a expressão de s acima, $3^3 2b(a - b)(a + b)$ é um cubo e portanto $2b(a - b)(a + b)$ é também um cubo. Os fatores dessa expressão são primos relativos e por isso $2b = \overline{x}^3, a - b = \overline{y}^3$ e $a + b = \overline{z}^3$. Por fim, $\overline{x}^3 = 2b = \overline{z}^3 - \overline{y}^3$ e temos $\overline{x}^3 + \overline{y}^3 = \overline{z}^3$. Se olharmos nossa trajetória, veremos que $\overline{z}^3 < z^3$, pois este é fator de fatores de z^3. Podemos então repetir todo o argumento para essa nova tripla e conseguir dessa forma uma sequência descendente infinita de número naturais $\overline{z}^3$, que é impossível. Para o caso $p^2 + 3q^2$ primos entre si, em suma os mesmos passos são utilizados e a mesma conclusão atingida. Logo, fica provado (com alguns detalhes em débito) que

[3] Aqui Euler utiliza o termo "irracional" não da maneira como hoje vemos: ele está se referindo aos números complexos

Teorema 4.1. *A equação $x^3 + y^3 = z^3$ não possui soluções inteiras não triviais.*

A inquietação trazida pelo argumento apresentado por Euler e tal generalização do Teorema Fundamental da Aritmética faz surgir um novo campo da Matemática, a Teoria Algébrica dos Números: para tratar de um problema sobre números inteiros nos dirigimos a um ambiente diferente (o corpo dos números complexos) e isso nos permitiu ter uma visão melhor de como lidar com a equação.

5. Uma nova esperança e o problema contra-ataca

Em uma correspondência a Goldbach (1690 - 1764), Euler, em 1753, observa que sua prova é bem diferente da resolução para $n = 4$. No decorrer dos séculos XVIII e XIX, demonstrações para casos específicos surgem: $n = 5$ recebe provas de Legendre (1752 - 1833) e Dirichlet (1805 - 1859), o caso $n = 14$ é resolvido por Dirichlet e $n = 7$ é devido a Gabriel Lamé (1795 - 1870). Uma grande contribuição nesse período vem de Sophie Germain (1776 - 1831).

Apesar de todas as dificuldades que enfrentou devido ao preconceito de gênero, Sophie (que assumia um pseudônimo masculino para se corresponder com outros matemáticos) tinha contato pessoal com Legendre em Paris e se comunicava por cartas com Carl Friedrich Gauss (1777 - 1855). No texto *Sobre alguns objetos de análise de equações e particulamente sobre o teorema de Fermat*[4], segundo complemento da obra *Ensaio sobre a Teoria dos Números* [5] (1825) de Legendre, Sophie é mencionada como responsável pelo seguinte resultado:

Se $x^5 + y^5 = z^5$, então um dos números x, y ou z deve ser divisível por 5,

que é facilmente generalizado como em [[EDWARDS], 1977, p.63]:

Teorema 5.1. *Se p é um primo ímpar tal que $2p + 1$ é primo, então $x^p + y^p = z^p$ implica que um dos números x, y ou z deve ser divisível por p.*

Isso permite olhar o Último Teorema de Fermat em dois casos:

Caso I: Nenhum dos números x, y e z é divisível por p;

Caso II: Um e apenas um entre x, y e z é divísivel por p (se dois deles o forem, isso implica o terceiro também ser divisível e poderíamos fatorar p, caindo em apenas um deles ser divisível ou o Caso I).

O Caso I é resolvido para os primos p na condição de que $2p + 1$ seja primo, olhando a contrapositiva da generalização do resultado de Sophie e podemos ainda extender para outros primos com outras condições análogas, como 7, que não atende a condição $2p + 1$ (pois $2 \cdot 7 + 1 = 15$), mas atende $4p + 1 = 29$. Mais uma vez, uma generalização nos leva ao Teorema de Sophie Germain:

Teorema 5.2. *Seja p primo ímpar. Se existe um primo auxiliar q com as propriedades*

- $x^p + y^p + z^p \equiv 0 \,(mod\, q) \Rightarrow x \equiv 0$ *ou* $y \equiv 0$ *ou* $z \equiv 0 \,(mod\, q)$ *e*
- $x^p \equiv p \,(mod\, q)$ *é impossível.*

Então o Caso I do Último Teorema de Fermat é verdadeiro para p.

[4]Sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat, tradução do autor
[5]Essai sur la Théorie des Nombres, tradução do autor

Sophie foi capaz de provar o Caso I para todos os primos ímpares menores que 100 e Legendre incluiu na lista os primos ímpares menores que 197 e outros.

Mesmo com os diversos casos particulares provados, não havia muita perspectiva de como se atacar a equação em sua forma geral. As demonstrações particulares, que em essência lidam com aritmética de números, eram sempre distintas e não davam margem para uma generalização.

Em 1845, porém, acontece um anúncio que, por alguns meses, mobiliza a comunidade matemática de Paris e traz uma nova esperança: Lamé afirma ter resolvido o problema. A estratégia utilizada era criativa, utilizando as raízes da unidade e explorando subconjuntos do corpo dos números complexos chamados corpos ciclotômicos para, a partir da fatoração

$$x^n + y^n = (x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{n-1} y),$$

utilizar o Princípio da Descida Infinita, com $\zeta = e^{\frac{2\pi i}{n}} = cos(\frac{2\pi}{n}) + isen(\frac{2\pi}{n})$. No entanto, o problema contra-ataca, pois novamente assumiu-se a generalidade do Teorema Fundamental da Aritmética e dessa vez erroneamente (pois é, ele não vale em qualquer situação), o que desqualificou a prova de Lamé.

O responsável por notar a falha no argumento foi o alemão Eduard Kummer (1810 - 1893), que havia estudado tais conjuntos anos antes e, propondo uma nova teoria, resolveu o Último Teorema de Fermat para uma classe de primos, denominados primos regulares, que tornava a afirmação geral (Caso I e II) de Fermat verdadeira para todos os primos menores que 100 exceto 37,59 e 67. É interessante notar que a resolução de Kummer nasce do estudo de um problema de Teoria dos Números bem diferente (as questões sobre reciprocidade de ordem superior).

Após os avanços de Kummer, que solidificam a recém nascida Teoria Algébrica dos Números, o problema estagnou-se, pois os casos particulares exigiam contas absurdamente complicadas e sem muito adicional teórico.

6. A conclusão de uma saga: a demonstração de Wiles

Mais de 140 anos após o trabalho de Kummer, o britânico natural de Cambridge Andrew Wiles (1953-) dá um desfecho para nossa história. Temos uma nova visão do problema: o estudo das chamadas curvas elípticas $y^2 = Ax^3 + Bx^2 + Cx + D$ $(A, B, C, D \in \mathbb{Q})$ junto com as funções modulares (certas funções complexas utilizadas em Teoria Analítica dos Números). O Último Teorema de Fermat ganha então um caráter geométrico. Wiles, que era um apaixonado pelo teorema desde os 10 anos de idade, trabalhou em uma conjectura da Geometria Algébrica, a Conjectura de Taniyama-Shimura-Weil, que implicaria o resultado esperado. Após 7 anos de estudos secretos, Wiles faz, em 1993, o anúncio de que havia vencido a equação de Fermat. Mas, não era ainda o momento: é encontrada uma falha na prova. Juntando-se então com Richard Taylor (1962 -), a falha é corrigida e a demonstração definitiva é entregue em outubro de 1994 para análise e publicada em maio de 1995, em dois artigo que juntos totalizam mais de 120 páginas! Em [[STEWART]], Capítulo 14, encontramos uma boa introdução às curvas e funções elípticas e um esboço da prova feita por Wiles na Seção 14.7, p.262. Wiles recebeu vários prêmios e reconhecimento midiático. Estava então completa uma saga de 358 anos.

Referências

[EDWARDS] , HAROLD M. Fermat's Last Theorem A Genetic Introduction to Algebraic Number Theory, Nova York: Springer-Verlag, 1977. 410 p. (Graduate Texts in Mathematics 50)

[KNEŽEVIC; KRTINIĆ] . A Note on Infinite Descent Principle, **The Teaching of Mathematics**, Belgrado, v.26, p. 67-78, 2013.

[STEWART] , DAVID IAN. Algebraic Number Theory and Fermat's last theorem, 3ª Edição, Massachusetts: AK Peters, 2002. 313 p.