Revista Brasileira de História da Matemática - Vol. 9 nº 17 (abril/2009 -setembro/2009) – pág. 93-99
Publicação Oficial da Sociedade Brasileira de História da Matemática
ISSN 1519-955X

"DEMONSTRAÇÃO DE CERTOS TEOREMAS REFERENTES A NÚMEROS PRIMOS", DE LEONHARD EULER: TRADUÇÃO E COMENTÁRIOS

Carlos H. B. Gonçalves
USP – Brasil

Thomás A. S. Haddad
USP – Brasil

(aceito para publicação em junho de 2008)

Resumo

Apresentamos neste trabalho uma tradução para a língua portuguesa de um importante texto de Leonhard Euler ("Theorematum quorundam ad numeros primos spectantium demonstratio"), lido perante a Academia de Ciências de São Petersburgo em 1736 e publicado em 1741 nos seus anais, contendo uma demonstração do chamado pequeno teorema de Fermat, um resultado fundamental em teoria dos números.

Palvras-chave: pequeno teorema de Fermat, números primos, Leonhard Euler.

Abstract

We present in this work a translation to Portuguese of an important text by Leonhard Euler ("Theorematum quorundam ad numeros primos spectantium demonstratio"), read at the Academy of Sciences of Saint Petersburg in 1736 and published in 1741 in the Academy proceedings, containing a proof of the so-called Fermat's little theorem, a fundamental result in number theory.

Key words: Fermat's little theorem, prime numbers, Leonhard Euler.

Introdução

O texto de Euler que traduzimos e comentamos a seguir contém uma demonstração do chamado pequeno teorema de Fermat. Um resultado fundamental da teoria dos números e da aritmética modular, bem com uma das portas de entrada para os

estudos de álgebra abstrata, o pequeno teorema afirma que, sendo p um número primo e a um inteiro qualquer (não divisível por p), então $a^{p-1} - 1$ é divisível por p. Ele está na base do teste de primalidade de Fermat e do método RSA de criptografia e pode ser generalizado para corpos finitos abstratos; no início do século XIX, Sophie Germain encontrou uma conexão entre este e o celebrado último teorema de Fermat. Originalmente, Pierre de Fermat o enunciou em uma carta a Frénicle de Bessy, em 18 de outubro de 1640.[1] Ainda que Leibniz tenha deixado uma demonstração completa do teorema em um manuscrito não-datado (mas necessariamente anterior ao período de atividade de Euler), a primeira prova efetivamente publicada é a que consta do texto aqui traduzido (Weil 1984, p. 56).

Em outro trabalho, abordamos questões relativas ao ensino da matemática e à história da disciplina que podem ser estimuladas a partir desse texto de Euler (Gonçalves e Haddad 2008). No presente trabalho, porém, nosso foco é a própria leitura do texto de Euler, com atenção aos problemas de tradução que essa fonte para a história da matemática pode trazer.

Antes da leitura do artigo de Euler, cabe destacar o emprego dado por ele ao termo "indução", que retém, em seu texto, o significado original de forma inferencial não-dedutiva, isto é, a intuição de uma verdade geral a partir de casos particulares (uma verdade não-necessária, deve-se salientar). O uso corrente do termo na matemática resultou em uma confusão, pois a indução de que se fala nas demonstrações matemáticas é um procedimento lógico de dedução de verdades necessárias (sendo um dos antecedentes do silogismo o próprio princípio de indução finita). Na seção introdutória do texto, Euler afirma que muitos dos enunciados de Fermat foram obtidos a partir de induções na acepção própria da palavra, e admite ser esse o fundamento mesmo do processo criativo na matemática. No entanto, ele critica severamente a falta de demonstrações completas, aludindo ao engano do próprio Fermat com relação a muitos enunciados em que depositou confiança apenas por tê-los tirado de inferências indutivas. Nesse sentido, o texto de Euler parece ser um testemunho de um ponto de inflexão importante na história da teoria dos números e da álgebra, que, à época da escrita, ainda se encontravam distantes dos padrões de rigor próprios da tradição geométrica, que viriam a se tornar predominantes.

"Demonstração de Certos Teoremas Referentes a Números Primos", de Leonhard Euler

1. Por vezes, muitos teoremas aritméticos de Fermat foram exibidos para o público, mas sem demonstrações, nos quais, se verdadeiros fossem, não só estariam contidas propriedades notáveis dos números, mas também a própria ciência dos números, que grandemente é vista exceder os limites da análise, fortemente seria promovida. Por mais, entretanto, que esse insigne geômetra mantivesse, a respeito de grande número de teoremas que propôs, ou poder demonstrá-los ou pelo menos estar certo da verdade deles, ainda em

[1] Fermat, como em outras ocasiões, enuncia o resultado sem uma demontração, alegando falta de espaço para tanto: "Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long." (Fermat 1894, 209)

lugar nenhum, o quanto me consta, expôs as demonstrações. Ora, o grande Fermat parece ter compreendido a maior parte de seus teoremas numéricos por indução, tanto que ele parecia abrir as propriedades que deviam ser extraídas quase por via única desse modo. Mas em verdade quão pouco pode ser atribuído às induções nesse assunto, (como) eu poderia mostrar por muitos exemplos; desses, todavia, seja suficiente trazer um único produzido pelo próprio Fermat. Falo, não é de se espantar, daquele teorema, cuja falsidade, já há um certo número de anos, pus à vista[2], pelo qual Fermat afirmou que todos os números compreendidos pela forma $2^{2^n} + 1$ são números primos. Todavia, para se convencer da verdade dessa proposição, parece ser completamente suficiente uma indução. Pois, exceto pelo fato que todos esses números menores do que 100000 sejam de fato primos, pode também ser facilmente demonstrado que nenhum número primo não excedente a 600 mede[3] esta fórmula $2^{2^n} + 1$, ainda que seja substituído o n por um número tão grande quanto se queira. Entretanto, mesmo que seja coisa assente que esta proposição não é conforme à verdade, facilmente entende-se o quanto a indução vale em especulações desse modo.

2. Por essa razão, todas as propriedades dessa natureza dos números que se apóiam somente na indução, por muito tempo julgo serem as que se devem ter na incerteza, até que elas ou sejam defendidas por evidentes demonstrações ou totalmente refutadas. Não julgaria, também, que se deve confiar mais naqueles teoremas que eu mesmo expus apressadamente naquele [trabalho][4] em que tratei do lembrado teorema fermatiano e de números perfeitos, se repousassem somente nas induções, bem a única via pela qual cheguei naquele tempo ao entendimento deles. Mas agora, uma vez que alcancei demonstrações firmíssimas desses teoremas por um método peculiar, não se deve mais duvidar da verdade deles. Por conseguinte, tanto pela verdade daqueles teoremas, a ser demonstrada, como pelo próprio método, com o qual cheguei às demonstrações, a ser exposto, que fortemente também em outras investigações de números poderá ter utilidade, nesta dissertação decidi explicar minhas demonstrações.

3. A proposição, então, que aqui tomei para ser demonstrada, é a seguinte:

Significando p um número primo, a fórmula $a^{p-1} - 1$ *sempre poderá ser dividida por p, a menos que a possa ser dividido por p.*

De fato, a partir desta proposição demonstrada, a verdade dos teoremas restantes flui espontaneamente. Um certo caso da fórmula proposta, para o qual $a = 2$, já dei demonstrado há algum tempo; entretanto ainda não pude estender a demonstração para a fórmula geral.

[2] Euler refere-se aqui a seu "Observationes de theoremate quodam Fermatiano, aliisque ad numeros primos spectantibus" (Observações sobre um Certo Teorema Fermatiano e sobre Outros que Dizem Respeito a Números Primos). Nesse trabalho (E26), Euler mostra que o quinto número de Fermat $2^{2^5}+1 = 4\ 294\ 947\ 297$ não é primo, pois é divisível por 641.

[3] O conceito de "medir" remonta à tradição aritmética da Antiguidade. Euler o usa duas vezes nesse texto. Equivale a "dividir".

[4] Trata-se do já mencionado E26.

Por essa razão, convém, em primeiro lugar, conduzir a verificação daquele caso pelo qual mais facilmente o trânsito para (coisas) mais gerais do que ele pode ser produzido. A ser demonstrada, então, será a proposição seguinte:

Significando p um número primo ímpar qualquer, a fórmula $2^{p-1} - 1$ *sempre poderá ser dividida por p.*

DEMONSTRAÇÃO

No lugar de 2, seja posto 1 + 1, e será

$$(1+1)^{p-1} = 1 + \frac{p-1}{1} + \frac{(p-1)(p-2)}{1\cdot 2} + \frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3} +$$

$$\frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4} + \text{etc.},$$ [5]

de cuja série[6] o número de termos é = p e, portanto, ímpar.[7] Além disso, qualquer termo, ainda que tenha aspecto de fração, dará um número inteiro; de fato, cada numerador, como é suficientemente claro, pode ser dividido por seu denominador. Então a série com o primeiro termo removido será

$$(1+1)^{p-1} - 1 = 2^{p-1} - 1$$

$$= 1 + \frac{p-1}{1} + \frac{(p-1)(p-2)}{1\cdot 2} + \frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3} + \frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4} + \text{etc.},$$

o número dos quais é = $p - 1$ e, por isso, par. Então agrupam-se cada dois termos em uma soma, com o que o número de termos faça-se o duplo menor[8]; será

$$2^{p-1} - 1 = \frac{p(p-1)}{1\cdot 2} + \frac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4}$$

$$+ \frac{p(p-1)(p-2)(p-3)(p-4)(p-5)}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6} + \text{etc.},$$

de cuja série o último termo, por causa do número ímpar p, será

$$\frac{p(p-1)(p-2)...2}{1\cdot 2\cdot 3...(p-1)} = p$$

[5] Euler usa tanto a abreviação "etc" como reticências para indicar termos que não estão explicitamente escritos. Enquanto a primeira é usada no final de expressões, as outras aparecem no interior das mesmas.
[6] As *séries* de Euler podem ter apenas um número finito de termos.
[7] Vemos nesse trecho um uso mais livre do sinal da igualdade, que aparece no meio do texto com o valor da expressão "igual a".
[8] Isto é, a metade.

Mas é evidente que os termos individuais são divisíveis por p; pois, como p é número primo e maior do que qualquer fator dos denominadores, em nenhuma parte poderá ser eliminado pela divisão. Por essa razão, se p for um número primo ímpar, $2^{p-1} - 1$ sempre poderá ser dividida por ele. C.Q.D.[9]

DE OUTRO MODO

Se $2^{p-1} - 1$ pode ser dividida por um número primo p, também seu dobro $2^p - 2$ poderá ser dividido e reciprocamente. De sua parte, é

$$2^p = (1+1)^p = 1 + \frac{p}{1} + \frac{p(p-1)}{1\cdot 2} + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3} + \ldots + \frac{p}{1} + 1$$

Cuja série, truncada do primeiro e último termos, dá

$$\frac{p}{1} + \frac{p(p-1)}{1\cdot 2} + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3} + \ldots + p = 2^p - 2$$

É claro, também, que qualquer termo dessa série é divisível por p, uma vez que p é número primo. Por essa razão, também $2^p - 2$ sempre poderá ser dividida por p e, por causa disso, também $2^{p-1} - 1$ por p, a menos que seja $p = 2$. C.Q.D.

4. Como, então, $2^{p-1} - 1$ pode ser dividida pelo número primo ímpar p, é fácil entender que também esta fórmula $2^{m(p-1)} - 1$ pode ser dividida por p, denotando m um número inteiro qualquer. Por isso, também as fórmulas seguintes todas $4^{p-1} - 1$, $8^{p-1} - 1$, $16^{p-1} - 1$ etc. poderão ser divididas pelo número primo p. Está, então, demonstrada a verdade do teorema geral para todos os casos, nos quais a é qualquer potência de dois[10] e p qualquer número primo além de dois[11].

5. Tendo demonstrado agora aquele teorema, com a ajuda dele demonstraremos também o seguinte

TEOREMA

Denotando p um número primo qualquer além do 3, esta fórmula $3^{p-1} - 1$ *sempre poderá ser dividida por ele.*

[9] No original, "Q.E.D.". A tradição em língua portuguesa apresenta a expressão "Como queríamos demonstrar" como uma substituta para a expressão latina "Quod erat demonstrandum", cuja tradução mais literal é "o que era necessário demonstrar."
[10] Em latim, "quaevis binarii potestas", isto é, "qualquer potência do [número] binário".
[11] Novamente, "praeter binarium", isto é, "exceto o [número] binário".

DEMONSTRAÇÃO

Se $3^{p-1} - 1$ pode ser dividida por um número primo p exceto 3, então $3^p - 3$ pode ser dividida por p, desde que p seja um número primo qualquer, e reciprocamente. É verdade que

$$3^p = (1+2)^p = 1 + \frac{p}{1}\cdot 2 + \frac{p(p-1)}{1\cdot 2}\cdot 4 + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}\cdot 8 + \ldots + \frac{p}{1}\cdot 2^{p-1} + 2^p,$$

de cuja série os termos individuais exceto o primeiro e o último poderão ser divididos por p, uma vez que p é número primo. Então pode ser dividida por p esta fórmula $3^p - 2^p - 1$, que é igual a esta

$$3^p - 3 - 2^p + 2.$$

Mas $2^p - 2$ sempre pode ser dividida pelo número primo p; então também $3^p - 3$. Por isso, $3^{p-1} - 1$ sempre pode ser dividida pelo p, desde que p seja um número primo exceto 3. C.Q.D.

6. Do mesmo modo, será possível progredir a partir deste valor do próprio a para o seguinte, maior por uma unidade. Mas porque quero produzir uma demonstração mais elegante e mais genuína do teorema geral, exponho o seguinte[12]

TEOREMA

Denotando p um número primo, se $a^p - a$ pode ser dividida por p, então também a fórmula $(a + 1)^p - a - 1$ poderá ser dividida pelo mesmo p.

DEMONSTRAÇÃO

Seja resolvida $(1 + a)^p$ conforme o costume em série; será

$$(1+a)^p = 1 + \frac{p}{1}\cdot a + \frac{p(p-1)}{1\cdot 2}\cdot a^2 + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}\cdot a^3 + \ldots + \frac{p}{1}\cdot a^{p-1} + a^p,$$

de cuja série os termos individuais, exceto o primeiro e o último, podem ser divididos por p, uma vez que p é um número primo. Por essa razão, $(1 + a)^p - a^p - 1$ admite[13] a divisão por

[12] Até esse ponto, a exposição de Euler indica a possibilidade de aplicar os mesmo procedimentos para demonstrar a validade da proposição para uma base a qualquer. Essa indicação de uma possibilidade de demonstrar a generalidade é presente também nos textos de aritmética da Antiguidade, como nos *Elementos* de Euclides. A partir desse ponto do texto, porém, Euler aborda a problemática da demonstração por outro mecanismo, que é o "método peculiar" que ele mencionou no parágrafo 1. Como se pode ver do texto que segue, tal método peculiar é o princípio da indução finita, com aplicação da indução na variável a.

[13] "admite a divisão por p", isto é, é divisível por p.

p; mas esta fórmula é congruente[14] com esta $(1 + a)^p - a - 1 - a^p + a$. Mas $a^p - a$ por hipótese pode ser dividida por p, logo também $(1 + a)^p - a - 1$. C.Q.D.

7. Como, então, dado que $a^p - a$ pode ser dividida pelo número primo p, também esta fórmula $(a + 1)^p - a - 1$ admite a divisão por p, segue-se também que $(a + 2)^p - a - 2$, e mesmo $(a + 3)^p - a - 3$ e genericamente $(a + b)^p - a - b$ podem ser divididas por p. Dado ainda $a = 2$, como já demonstramos que $2^p - 2$ pode ser dividida por p, é claro que a fórmula $(b + 2)^p - b - 2$ deve admitir a divisão por p, qualquer que seja o número inteiro substituído no lugar de b.

Então p mede a fórmula $a^p - a$ e, conseqüentemente, também esta $a^{p-1} - 1$, a menos que seja $a = p$ ou múltiplo do próprio p. E essa é a demonstração do teorema geral, que tomei para apresentar.

Referências

Euler, Leonhard. 1741. "Theorematum quorundam ad numeros primos spectantium demonstratio". *Commentarii academiae scientiarum Petropolitanae*, vol. 8, 141-146. Também em *Opera Omnia*, Series 1, volume 2, 33-37 (Índice de Eneström 54).

Fermat, Pierre de. 1894. "Léttre XLIV. Fermat a Frénicle, Jeudi 18 Octobre 1640". In: Paul Tannery e Charles Henry (eds.). *Ouevres de Fermat. Tome 2éme: Correspondance*. Paris: Gauthier-Villars (pp. 206-212).

Gonçalves, Carlos H. B. e Haddad, Thomás A. S. 2008. "A Demonstração de Euler do Pequeno Teorema de Fermat: Usos Didáticos e Questões Historiográficas". In: E. R. Pacheco e W. R. Valente (eds.). *Anais do VII Seminário Nacional de História da Matemática*, Sociedade Brasileira de Matemática (pp. 199-201).

Weil, André. 1984. *Number Theory: An Approach through History from Hammurapi to Legendre*. Boston: Birkhäuser.

[14] Não se trata aqui da congruência módulo m, como seria depois sistematizada por Gauss. Ao afirmar que duas expressões são congruentes, Euler quer simplesmente dizer que são iguais.

Carlos H. B. Gonçalves
Escola de Artes, Ciências e Humanidades da Universidade de São Paulo

E-mail: bgcarlos@usp.br

Thomás A. S. Haddad
Escola de Artes, Ciências e Humanidades da Universidade de São Paulo

E-mail: thaddad@usp.br