NOTA DE AULA

Sobre um teorema de Lucas relacionado com o pequeno teorema de Fermat

por José Morgado
Instituto de Matemática, Universidade Federal de Pernambuco, Brasil

1. O pequeno teorema de FERMAT estabelece que, para todo inteiro racional a não divisível pelo inteiro racional primo positivo p, é válida a congruência

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

No entanto, como é bem sabido, do facto de a congruência

$$a^{n-1} \equiv 1 \pmod{n}$$

ser válida para algum inteiro racional a (necessàriamente primo com n), não se pode concluir que o inteiro racional positivo n seja primo. Assim, como foi observado por F. SARRUS em 1819 [1], tem-se

$$2^{340} \equiv 1 \pmod{341},$$

apesar de $341 (= 11.31)$ não ser primo.

Em 1876, ÉDOUARD LUCAS obteve o seguinte resultado [2]:

Se n *é um inteiro racional positivo tal que, para algum inteiro racional* a, *se tem*

$$\mathrm{a}^{\mathrm{n}-1} \equiv 1 \pmod{\mathrm{n}}$$

e, para todo inteiro racional t *satisfazendo à condição* $0 < \mathrm{t} < \mathrm{n} - 1$, *se tem*

$$\mathrm{a}^{\mathrm{t}} \not\equiv 1 \pmod{\mathrm{n}},$$

então n *é primo.*

Posteriormente, em 1891, E. LUCAS [3] melhorou este resultado, estabelecendo que:

Se a congruência

$$\mathrm{a}^{\mathrm{x}} \equiv 1 \pmod{\mathrm{n}}$$

é válida para $\mathrm{x} = \mathrm{n} - 1$, *mas não é válida se* x *é divisor próprio de* $\mathrm{n} - 1$, *então* n *é primo.*

Nesta nota, formulamos um análogo a etse teorema de LUCAS, para anéis comutativos.

2. Seja A um anel comutativo e seja P um ideal próprio de A.

Recordemos que P se diz um ideal primo de A, se é satisfeita a seguinte condição:

Se $\mathrm{x}, \mathrm{y} \in \mathrm{A}$ *e* $\mathrm{xy} \in \mathrm{P}$, *então* $\mathrm{x} \in \mathrm{P}$ *ou* $\mathrm{y} \in \mathrm{P}$.

Recordemos ainda que, se A é um anel comutativo com elemento um, então o ideal P de A é um ideal primo, se e só se o anel quociente A/P é um domínio de integridade.

Um análogo ao pequeno teorema de FERMAT para anéis comutativos pode enunciar-se assim:

TEOREMA 1. *Se* A *é um anel comutativo com elemento um e* P *é um ideal primo de* A

tal que o anel quociente A/P *tem precisamente* n *elementos, então tem-se*

$$(a + P)^{n-1} = 1 + P$$

ou, equivalentemente,

$$a^{n-1} \equiv 1 \pmod{P},$$

para todo elemento a *de* A *que não pertença a* P.

Dem.: Com efeito, da circunstância de A/P ser um domínio de integridade finito, conclui-se que A/P é um corpo e, por isso, os seus elementos não nulos constituem um grupo multiplicativo cuja ordem é $n-1$.

Para todo elemento $a \in A$ tal que $a \notin P$ tem-se, por consequência,

$$a^{n-1} + P = (a + P)^{n-1} = 1 + P,$$

como se pretendia.

O pequeno teorema de FERMAT, na sua forma original, é justamente um caso particular deste teorema, a saber, o caso em que o anel A é o anel Z dos inteiros racionais. Então um ideal primo P de A é o ideal principal gerado por um inteiro racional positivo primo p e o anel quociente A/P tem exactamente p elementos.

O teorema anterior mostra que o pequeno teorema de FERMAT é válido no anel dos inteiros de GAUSS $G = \{a + ib : a, b \in Z\}$ ([4], pp. 19-21) (em anéis de inteiros algébricos ver [4], pp. 109-110).

3. Vamos agora estabelecer, para anéis comutativos, um teorema análogo ao teorema de LUCAS, tal como foi formulado em [3].

TEOREMA 2. *Seja* A *um anel comutativo com elemento um e seja* P *um ideal de* A *tal que o anel quociente* A/P *tem* n *elementos. Se, para algum* $a \in A$, *se tem*

$$(a + P)^{n-1} = 1 + P$$

e se, para todo divisor próprio t *de* $n-1$, *se tem*

$$(a + P)^t \neq 1 + P,$$

então P *é um ideal primo de* A.

Dem.: Na verdade, consideremos os seguintes elementos de A/P:

$$(1) \quad P, a+P, a^2+P = (a+P)^2, \cdots, a^{n-1} + P = (a+P)^{n-1}.$$

É fácil ver que, se $i, j \in \{1, 2, \cdots, n-1\}$, então

$$(2) \quad i \neq j \text{ implica } a^i + P \neq a^j + P.$$

Com efeito, suponhamos que

$$(3) \quad a^i + P = a^j + P$$

tendo-se, por exemplo, $i > j$.

Ora, fazendo $n - 1 - i = k$, de (3) resultaria

$$a^{n-1} + P = a^{i+k} + P = a^{j+k} + P$$

e, como, por hipótese,

$$a^{n-1} + P = 1 + P,$$

ter-se-ia

$$a^{j+k} \in 1 + P$$

com $0 < j + k < n - 1$.

Designemos por d o menor inteiro racional positivo tal que

$$a^d \in 1 + P$$

e vejamos que, então, d é divisor de $n-1$.

De facto, pelo algoritmo de divisão,

$$n - 1 = dm + r \quad \text{com} \quad 0 \leq r < d$$

e, por consequência,

$$1+P=a^{n-1}+P=(a+P)^{n-1}=(a+P)^{dm+r}=$$
$$=(a^d+P)^m\cdot(a^r+P)=(1+P)^m\cdot$$
$$\cdot(a^r+P)=(1+P)\cdot(a^r+P)=a^r+P,$$

isto é,

$$a^r \text{ e } 1+P,$$

donde, pela definição de d, resulta que $r=0$, quer dizer, d é divisor de $n-1$.

Mas, como

$$d \leqq j+k<n-1,$$

não pode ter-se, por força da hipótese, $(a+P)^d=1+P$.

Esta contradição mostra a validade da implicação (2).

Assim, em (1) estão precisamente os n elementos que constituem o anel A/P. Então o conjunto dos elementos de A/P que são diferentes de P constitui um grupo abeliano (cíclico), com respeito à multiplicação do anel A/P.

Isto significa que o anel A/P é um corpo, logo, um domínio de integridade e, portanto, P é um ideal primo, como queríamos mostrar.

BIBLIOGRAFIA

[1] O. Ore, *Number Theory and its History*, Mc Graw-Hill Book Company, Inc., New York, 1948.

[2] L. E. Dickson, *History of the Theory of Numbers*, vol. 1, Chelsea Publ. Company, New York, 1952.

[3] E. Lucas, *Théorie des Nombres*, tome premier, nouveau tirage, Librairie Scientifique et Technique Albert Blanchard, Paris, 1961.

[4] H. Pollard, *The Theory of Algebraic Numbers*, The Carus Mathematical Monographs, No. 9, John Wiley and Sons, Inc., third impression, 1965.