# Fatoração de Polinômios do Anel de Séries Formais de Potências com Coeficientes Inteiros

De Bona, T. G.[1], Sant'Anna, A. A.[2]

1 Thayner Gomes De Bona , Bacharelado em Matemática, UFRGS
2 Alveri Alves Sant'Anna

UFRGS PROPESQ XXV SIC Salão Iniciação Científica
CET - Ciências Exatas e da Terra

## Redutibilidade em Z[[X]]

O anel de séries formais de potências com coeficientes inteiros é um domínio de fatoração única, isto é, todo elemento não inversível ou é irredutível ou pode ser escrito como produto de irredutíveis. Sendo assim, estamos interessados em estudar a redutibilidade de polinômios neste domínio. Alguns casos são simples, e estão resumidos a seguir

**Teorema.** *Seja* $f(X) = a_0 + a_1X + \cdots + a_dX^d \in Z[[X]]$. *Então:*
*(i) Se* $a_0 = \pm 1$, *então* $f(X)$ *é inversível;*
*(ii) Se* $a_0 = p$ *é primo, então* $f(X)$ *é irredutível;*
*(iii) Se* $a_0 = mn$, *com* $m \neq \pm 1 \neq n$ *e* $\mathrm{mdc}(m,n) = 1$, *então* $f(X)$ *é redutível;*
*(iv) Se* $a_0 = p^n$, *com* $p$ *primo e* $n > 1$, *e* $\mathrm{mdc}(p, a_1) = 1$, *então* $f(X)$ *é irredutível.*

Todos estes casos são verificáveis através da análise dos coeficientes das séries numa possível fatoração de $f(X)$. É importante observar que fatoração em $Z[X]$ e $Z[[X]]$ não tem qualquer relação direta. De fato, o polinômio $6 + X + X^2$ é irredutível em $Z[X]$, mas pode ser fatorado em $Z[[X]]$. Por outro lado, o polinômio $2 + 7X + 3X^2$ admite a fatoração $(2 + X)(1 + 3X)$ em $Z[X]$, porém esta não é uma fatoração própria em $Z[[X]]$, visto que um dos fatores é inversível.

Com os resultados do Teorema, vê-se que falta somente considerar o caso em que $f(X)$ é da forma

$$f(X) = p^n + p^m a_1 X + a_2 X^2 + \cdots + a_d X^d$$

com $a_d$ não nulo, $n > 1, m > 1$, e $\mathrm{mdc}(p, a_1) = 1$. Separamos este caso em dois: quando $n > 2m$ e quando $n \leq 2m$.

## Inteiros *p*-ádicos

Estamos acostumados a trabalhar no conjunto dos números inteiros com a métrica euclidiana, que nos é mais natural. Porém, há outras métricas interessantes que podem ser definidas em $Z$. Fixado um número primo $p$, dizemos que a maior potência de $p$ que divide um certo número inteiro $n$ é á *valorização p-ádica* de $n$, e denotamos este número por $v_p(n)$. Com esta notação, a função

$$d(m,n) = \frac{1}{p^{v_p(m-n)}}$$

define uma métrica em $Z$. O interessante aqui é que existem sequências de Cauchy nesta métrica que não convergem em $Z$, de modo que faz sentido falarmos no completamento métrico de $Z$ com relação a métrica $d$, e é a este conjunto que damos o nome de números inteiros $p$-ádicos, denotado por $Z_p$. Podemos estender naturalmente a soma e o produto de $Z$ a $Z_p$, obtendo assim um domínio de integridade. Trazemos aqui alguns resultados importantes sobre $Z_p$ e $Z_p[X]$:

**Teorema.** *Sejam* $a \in Z_p$ e $f(X) \in Z[X]$.
*(i) Existem* $n = v_p(a)$ *e* $u \in Z_p$ *inversível tais que* $a = p^n u$;
*(ii)* $f(X)$ *possui uma raíz em* $Z_p$ *se, e somente se, possui uma raíz modulo* $p^k$, *para cada* $k \geq 1$;
*(iii) Se* $f(a) = 0 \pmod{p^{2\delta+1}}$, $f(a) = 0 \pmod{p^{\delta}}$ *e* $f'(a) \neq 0 \pmod{p^{\delta+1}}$ *para algum* $\delta \geq 1$, *então existe um único* $\theta \in Z_p$ *tal que* $f(\theta) = 0$ *em* $Z_p$ *e* $\theta = a \pmod{p^{\delta+1}}$.

Utilizando o Teorema acima, podemos encontrar, em alguns casos particulares, relações entre a redutibilidade de um polinômio com coeficientes inteiros em $Z[[X]]$ e $Z_p[X]$.

## REFERÊNCIAS BIBLIOGRÁFICAS

BIRMAJER, D.; GIL J.B. Arithmetic in the ring of formal power series with integer coefficients, *American Mathematical Monthly*, [S.l.], v. 115, p. 541-549, 2008.
BIRMAJER, D.; GIL, J. B.; WEINER, M. Factoring polynomials in the ring of formal power series over $Z$. *International Journal of Number Theory*, [S.l.], p. 1763-1776, 27 ago. 2012.
KATOK, S. Real and p-adic analysis course notes. Disponível em: http://www.personal.psu.edu/sxk37/pub/p-adic.pdf. Acesso em: 03 out. 2013.

25 anos
MODALIDADE DE BOLSA
PROBIC FAPERGS