Irredutibilidade módulo p de polinômios a duas variáveis

Mandio Pietro Gallas Duarte
Orientadora: Prof.ª Virgínia Maria Rodrigues

Introdução

Um polinômio a duas variáveis com coeficientes em um corpo F é **absolutamente irredutível** sobre F se ele é irredutível sobre qualquer extensão algébrica de F.

Exemplo:
$x^2 + 2xy + y^2 - 2$ é irredutível sobre $\mathbb{Q}$, mas não sobre $\mathbb{R}$,
$x^2 + 2xy + y^2 - 2 = (x + y - \sqrt{2}).(x+y+\sqrt{2})$

No entanto, a irredutibilidade absoluta de um polinômio com coeficientes racionais pode ser perdida módulo, *p* com *p* primo.

Em 1919, A. Ostrowski [2] provou que todo polinômio multivariado com coeficientes inteiros, absolutamente irredutível sobre $\mathbb{Q}$, permanece absolutamente irredutível módulo *p* para *p* primo suficientemente grande.

Desde então, diversos matemáticos estabeleceram cotas para primos que preservam a irredutibilidade absoluta. Em particular, para polinômios bivariados, destacamos:

- W. Ruppert [2], 1999:

$$p > [m(n+1)n^2+(m+1)(n+1)m^2]^{mn+(n-1)}.\ H(f)^{2mn+n-1},$$

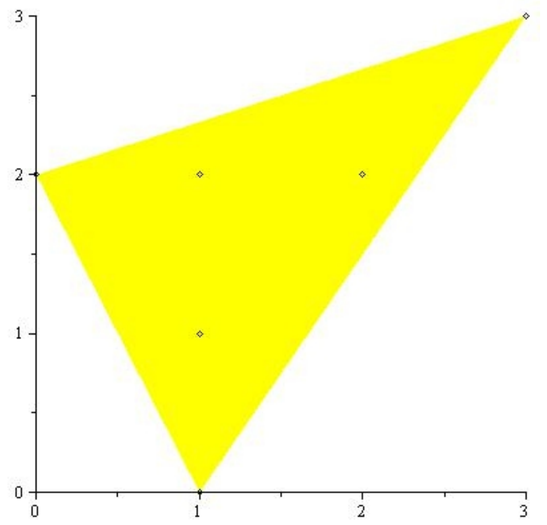
onde $H(f)$ é o maior dos coeficientes em módulo e $\deg(f)=(m,n)$, ou seja, m e n são os graus do polinômio em relação às variáveis x e y.

- S. Gao e V. Rodrigues [3], 2003:

$$p > (\sqrt{m^2+n^2}.\|f\|_2)^{2t-3}, \quad (1)$$

onde t é o número de pontos com coordenadas inteiras no politopo de Newton associado ao polinômio e $\|f\|_2$ é a sua norma euclidiana.

O **politopo de Newton** associado a um polinômio é o menor polígono convexo que contém os pontos do plano formados pelos expoentes de cada termo do polinômio.



Politopo de Newton de $x + y^2 + xy^2 + x^3y^3$

Desenvolvimento

Para obter a cota (1), Gao e Rodrigues utilizam um critério de irredutibilidade, para um polinômio $f \in F[x,y]$, baseado na existência de solução para a equação diferencial

$$\frac{\partial}{\partial y}\left(\frac{g}{f}\right)=\frac{\partial}{\partial x}\left(\frac{h}{f}\right) \quad (2)$$

onde $\deg(f)=(m,n)$, $\deg(g)=(m-1,n)$ e $\deg(h)=(m,n-1)$.

Esta equação pode ser reescrita como um sistema de equações lineares, cujas variáveis são os coeficientes de g e h.

Gao [4] determina que o número de fatores irredutíveis distintos de f sobre F é igual à dimensão do espaço solução de (2). Assim, basta que a matriz associada ao sistema linear possua posto ρ -1, onde ρ é o número de variáveis do sistema, para que o polinômio f seja absolutamente irredutível sobre F. Portanto, dado um primo *p*, para que f permaneça absolutamente irredutível módulo *p*, é suficiente que *p* seja maior que o determinante de todas as submatrizes de ordem ρ -1.

Resultados:

Neste trabalho, desenvolvemos um programa, na plataforma Maple, que, dado um polinômio bivariado com coeficientes inteiros, calcula o politopo de Newton associado, determina as cotas dadas por Rupert e por Gao e Rodrigues, constroi o sistema de equações lineares decorrente de (2) e, a partir da matriz associada a este sistema, determina os primos de risco.

Além disso, provamos que quando $t < m.n$, ou seja, quando o número de pontos com coordenadas inteiras do politopo de Newton é menor que o produto dos graus dos polinômio em relação as suas variáveis, a cota Gao-Rodrigues é necessariamente menor que a cota de Rupert.

Referências Bibliográficas:

[1] A. Ostrowski, Zur arithmetischen theorie der algebraischen grössen, *Nachr. K. Ges. Wiss*. Göttingen (1919), 273-298
[2] W. M. Ruppert, Reducibility of polynomials f(x, y) modulo p, J*ournal of Number Theory 77* (1999), 62-70.
[3] S. Gao e V. M. Rodrigues, Irreducibility of polynomials modulo p via Newton Polytopes, *Journal of Number Theory 101* (2003), 32-47
[4] S. Gao. Factoring multivariate polynomials via partial differential equations. *Mathematics of Computation 72* (2003), 801-822.