UFRGS

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA

Um Teste Determinístico de Primalidade

Introdução

Um teste determinístico de primalidade é um algoritmo que, tendo por entrada um número positivo *n*, determina se este *n* é ou não um número primo, com 100% de certeza. Apresentaremos nesta exposição um certo teste determinístico de primalidade, e discutiremos os aspectos da teoria de números que dão suporte ao algoritmo apresentado. Ao longo deste trabalho, *x* denotará uma variável e muitos dos cálculos serão efetuados em $Z_n[x]$, o anel dos polinômios com coeficientes em Z_n.

Teorema:

Sejam *n* e *b* inteiros positivos e primos entre si. Então,

$$(x+\bar{b})^n = x^n + \bar{b}^n \quad em \quad Z_n[x]$$

se, e somente se, *n* é primo.

A demonstração deste teorema depende de um resultado sobre números binomias que isolaremos no seguinte lema:

Lema:

Seja *n* um inteiro positivo. Então, *n* é primo se, e somente se,

$$\binom{n}{k} \equiv 0 \pmod{n}$$

Para todo $1 \leq k \leq n-1$

Podemos usar o teorema acima, para demonstrar o teorema de Fermat, ao qual está intimamente relacionado.

Teorema de Fermat:

Seja *p* um primo positivo e *b* um número inteiro. Se *p* não divide *b* então

$$b^{p-1} \equiv 1 \pmod{p}$$

Combinando o Teorema inicial com o Teorema de Fermat, obtemos o seguinte resultado, que desempenhará um papel chave para o nosso teste determinístico de primalidade.

Corolário:

Sejam *n* e *b* inteiros positivos primos entre si. Então, $(x+\bar{b})^n = x^n + \bar{b} \quad em \quad Z_n[x]$ se, e somente se, *n* é primo.

Note que a diferença entre o teorema inicial e o corolário acima é que b^n do lado direito da congruência passou a ser *b* no corolário. Podemos fazer esta troca, quando *n* é primo, por conta do teorema de Fermat. Por outro lado, se *n* não for primo, a troca não afeta o fato de haver números binomiais que não se anulam módulo *n*.

A expressão *teste de primalidade* refere-se a um algoritmo que, tendo por entrada um inteiro positivo *n*, determina se *n* é, ou não é, primo. Para obter um tal teste, precisamos de alguma propriedade que seja verdadeira se, e somente se, *n* é primo, e é exatamente isto que o corolário acima nos dá. Portanto, usando o corolário, podemos formular o seguinte teste.

Teste de primalidade determinístico

Entrada: inteiro positivo *n*

Saída: mensagem indicando se *n* é ou não primo.

Primeira etapa: Calcule todos os termos da expansão

$$(x+\bar{b})^n \ em \ Z_n[x]$$

Segunda etapa: Verifique se a expressão obtida na etapa anterior é igual a $x^n + \bar{b}$. Se for *n* é primo, se não for *n* é composto.

Exemplo:

1) Vamos determinar pelo teste acima se 7 é primo:

Tome x=3 e b=1, logo

$(3+1)^7 = 3^7 + 1 \ em \ Z_7$

$(3+1)^7 = 4^7 = 16384 \equiv 4 \ mod \ 7$

e $3^7 + 1 = 2187 + 1 = 2188 \equiv 4 \ mod \ 7$

Como 4=4, temos que 7 é primo.

2) Agora vamos determinar se 8 é primo:

Tome x=3 e b=1, logo

$(3+1)^8 = 4^8 + 1 \ em \ Z_8$

$(3+1)^8 = 4^8 = 65536 \equiv 0 \ mod \ 8$ e

$3^8 + 1 = 6561 + 1 = 6562 \equiv 1 \ mod \ 8$

Como $0 \neq 1$, temos que 8 não é primo.

OBS:

Será que podemos determinar se 8 é primo (exemplos 2 acima), tomando x=2 e b=1???

$(2+1)^8 = 2^8 + 1 \ em \ Z_8$

$(2+1)^8 = 3^8 = 6561 \equiv 1 \ mod \ 8$

e $2^8 + 1 = 256 + 1 = 257 \equiv 1 \ mod \ 8$

Como 1=1, temos que 8 é primo !!!!

Sabemos que isso é um absurdo. Mas então o que precisamos cuidar?

Pelo teorema de Fermat sabemos *x* não pode ser um divisor de zero módulo *n*. Logo *x* não pode ser igual a 2.

Portanto, para aplicar este teste de primalidade determinístico, precisamos cuidar que $mdc(n,b) = 1$ e que *x* não pode ser um divisor de zero módulo *n.*

Isto é o que chamamos de um *teste determinístico de primalidade*. Ele é *determinístico* porque, seja a resposta primo ou composto, temos a garantia que está correta. Mas por possuir um custo de execução exponencial ele é pouco usado, sendo trocado pelos testes Não determinísticos de primalidade que possui um custo polinomial, ou seja, o tempo de execução é inferior, mas que apenas garantem com uma certa probabilidade, a primalidade de um número.

Referência Bibliográfica

COUTINHO, S. C., **Primalidade em tempo Polinomial - Uma introdução ao Algoritmo AKS** - Rio de Janeiro, SBM, 2004.

Bolsista: Grasiela Martini – BIC - FAPERGS
Professor orientador: Alveri Alves Sant” Ana