Teorema Chinês do Resto e o Teorema de Euler-Fermat

Prof. Dr. Vinícius Wasques

Universidade Estadual Paulista "Júlio de Mesquita Filho" - Campus Rio Claro

22 de junho de 2020

Equações módulo n

Trataremos nessa aula equações da seguinte forma:

$$x \equiv b \ (mod \ n),$$

em que b e n são números inteiros dados e x é a variável a ser determinada.

Equações módulo n

Esse problema é simples, uma vez que as soluções são da forma:

$$x = b + kn,$$

para $k \in \mathbb{Z}$.

Já que

$$x \equiv \; b \, (mod \;\, n) \Leftrightarrow n | x - b \Leftrightarrow x - b = kn \Leftrightarrow x = b + kn,$$

para algum $k \in \mathbb{Z}$.

Exemplo:

Determine as soluções da equação modular

$$x \equiv 3 \ (mod\ 5).$$

Exemplo:

Determine as soluções da equação modular

$$x \equiv\ 3\ (mod\ 5).$$

Como $x \equiv\ 3\ (mod\ 5)$, então temos que $n|x-3$ e consequentemente $x = 3 + 5k$.

Isso implica que existem infinitas soluções em $\mathbb{Z}$ para esse problema.

No entanto, a solução é única módulo 5.

Sistemas de equação módulo n

Sistemas de equações modulares são mais elaborados:

$$\begin{cases} x \equiv \; b_1 \; (mod \; a_1) \\ x \equiv \; b_2 \; (mod \; a_2) \\ \quad \vdots \\ x \equiv \; b_m \; (mod \; a_m) \end{cases}$$

Isto é, uma solução para esse problema consiste em determinar um valor de $x \in \mathbb{Z}$ que satisfaz todas as equações modulares simultaneamente para $a_1, \ldots, a_m$ e $b_1, \ldots, b_m$ dados.

Exemplo:

Determine a solução do seguinte sistema modular

$$\begin{cases} x \equiv \ 1 \, (mod \; 11) \\ x \equiv \ 2 \, (mod \; 7) \end{cases}$$

Exemplo:

Determine a solução do seguinte sistema modular

$$\begin{cases} x \equiv \ 1 \ (mod \ 11) \\ x \equiv \ 2 \ (mod \ 7) \end{cases}$$

A primeira equação revela que $x = 1 + 11k$, para algum $k \in \mathbb{Z}$.

Agora sejam q e r o quociente e o resto da divisão de k por 7, respectivamente.

Assim, $k = 7q + r$.

Exemplo:

Substituindo k em x, obtemos

$$x = 1 + 11(7q + r) = 1 + 77q + 11r$$

Para x satisfazer a segunda congruência, devemos determinar $r \in \{0, 1, \ldots, 6\}$ tal que

$$11r + 1 \equiv \ 2(mod\ 7),$$

ou seja, $4r \equiv \ 1\ (mod\ 7)$ (verifique esse fato).

Como o inverso de 4 $(mod\ 7)$ é 2 (verifique esse fato), obtemos

$$r = 2 \quad \text{e portanto} \quad x = 77q + 23.$$

Teorema Chinês do Resto

Sejam $b_1, b_2, \ldots, b_k$ números inteiros quaisquer e $a_1, a_2, \ldots, a_k$ primos entre si dois a dois. Assim, o sistema de equações

$$\begin{cases} x \equiv \; b_1 \; (mod \; a_1) \\ x \equiv \; b_2 \; (mod \; a_2) \\ \quad \vdots \\ x \equiv \; b_m \; (mod \; a_m) \end{cases}$$

admite solução, que é única módulo $A = a_1.a_2 \ldots a_m$.

Demonstração

Consideremos os números

$$M_i = \frac{A}{ai} = a_1 \dots a_{i-1}.a_{i+1} \dots a_m$$

para todo $i \in \{1, \dots, m\}$.

Como $mdc(a_i, M_i) = 1$, então pela Proposição vista na última aula existe X_i inteiro tal que

$$M_i X_i \equiv \ 1 \ (mod \ a_i).$$

Demonstração

Note que se $j \neq i$, então $M_j = a_1 \dots a_{j-1}.a_{j+1} \dots a_m$ é múltiplo de a_i e portanto

$$M_j X_j \equiv \ 0 \ (mod \ a_i).$$

Assim, temos que

$$x_0 = M_1 X_1 b_1 + M_2 X_2 b_2 + \dots + M_m X_m b_m$$

é solução do sistema de equações, pois

$$x_0 \equiv \ M_i X_i b_i \equiv \ b_i \ (mod \ a_i).$$

para todo i.

Demonstração

Para mostrar que essa solução é única, suponha que exista uma outra solução x_1.

Assim,

$$x_0 \equiv \; x_1 \; (mod \; a_i) \Leftrightarrow a_i | x_0 - x_1.$$

para todo a_i.

Como todos os números a_i são dois a dois primos, temos que

$$A | x_0 - x_1 \Leftrightarrow x_0 \equiv \; x_1 \; (mod \; A)$$

mostrando a unicidade módulo A.

Exemplo:

Determine a solução do seguinte sistema modular

$$\begin{cases} x \equiv \ 1 \ (mod \ 11) \\ x \equiv \ 2 \ (mod \ 7) \end{cases}$$

Exemplo:

Determine a solução do seguinte sistema modular

$$\begin{cases} x \equiv \ 1 \ (mod \ 11) \\ x \equiv \ 2 \ (mod \ 7) \end{cases}$$

Pelo Teorema Chinês do resto, temos que: $A = 11.7 = 77$, $M_1 = 7$ e $M_2 = 11$.

Logo, existem X_1 e X_2 tais que

$$7X_1 \equiv \ 1 \ (mod \ 11) \quad \text{e} \quad 11X_2 \equiv \ 1 \ (mod \ 7)$$

Note que $X_1 = 8$ e $X_2 = 2$ são soluções (verifique esse fato)

Assim,

$$x_0 = M_1 X_1 b_1 + M_2 X_2 b_2 = 100$$

Portanto, as soluções do sistema linear são dadas por 100 módulo $A = 77$. Isto é, a solução do sistema linear é dada por

$$\overline{23} \in \mathbb{Z}_{77}$$

conforme havíamos constatado anteriormente $(x = 77q + 23)$.

Para resolver os sistema, precisamos determinar os valores de X_i tais que

$$M_i X_i \equiv 1 \ (mod \ a_i)$$

A fim de estudar esse problema, precisamos do conceito de função de Euler.

Função de Euler

Seja n um número inteiro positivo, a função de Euler, denotada por $\varphi(n)$, é definida como sendo o número de inteiros positivos menores ou iguais a n e que são relativamente primos com n.

Para essa função, temos que: (verifique os fatos abaixo)

- $\varphi(1) = \varphi(2) = 1$;
- $1 < \varphi(n) < n$ para qualquer $n > 2$;
- Se p é primo, então $\varphi(p) = p - 1$;
- Se p é primo, então $\varphi(p) = p - 1$;

Teorema de Euler-Fermat

Sejam a e m dois inteiros com $m > 0$ e $mdc(a, m) = 1$. Assim

$$a^{\varphi(m)} \equiv 1 \ (mod \ m).$$

Demonstração

Observe que se $r_1, r_2, \ldots, r_\varphi(m)$ é um sistema completo de invertíveis módulo m e a é um número natural tal que $mdc(a, m) = 1$, então

$$ar_1, ar_2, \ldots, ar_\varphi(m)$$

também é um sistema completo de invertíveis módulo m.

De fato, temos que $mdc(ar_i, m) = 1$ para todo i e se $ar_i \equiv\ ar_j\ (mod\ m)$, então $r_i \equiv\ r_j\ (mod\ m)$ pois a é invertível módulo m.

Logo, $r_i = r_j$ e portanto $i = j$. Consequentemente cada ar_i deve ser congruente com algum r_j.

Assim,

$$\prod_{1 \leq i \leq \varphi(m)} ar_i \equiv \prod_{1 \leq i \leq \varphi(m)} r_i \ (mod \ m)$$

se, e somente se

$$a^{\varphi(m)} \prod_{1 \leq i \leq \varphi(m)} r_i \equiv \prod_{1 \leq i \leq \varphi(m)} r_i \ (mod \ m.)$$

Como cada r_i é invertível módulo m, simplificando o fator

$$\prod_{1 \leq i \leq \varphi(m)} r_i$$

obtemos o resultado desejado

Pequeno Teorema de Fermat

Como corolário do Teorema de Euler-Fermat, temos:

$$a^{p-1} \equiv 1 \; (mod \; p),$$

para p primo tal que p não divide a.

Exercícios

a) Demonstre o Pequeno Teorema de Fermat e conclua que $a^p \equiv\ a\ (mod\ p)$

b) Utilize o Teorema de Euler-Fermat para mostrar a seguinte consequência

Se $mdc(a,m) = 1$, então a equação $ax \equiv\ b\ (mod\ m)$, tem solução única módulo m, dada por

$$x \equiv a^{\varphi(m)-1} b\ (mod\ m)$$

Como consequência temos que todas as soluções da equação $ax \equiv\ b \, (mod\ m)$ são da forma

$$x = a^{\varphi(m)-1}b + km$$

onde $k \in \mathbb{Z}$.

Referências

MARTINEZ, F.E.B; MOREIRA, C.G.T; SALDANHA, N.,T.; TENGAN, E. Teoria dos Números. Um passeio com Primos e outros Números Familiares pelo Mundo Inteiro. IMPA, 2013.

GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O
Matemática Concreta. LTC, São Paulo, 1995

NIVEN, I. E.; ZUCKERMAN, N.S. An Introduction to the Theory of Numbers, NY, John Wiley & Sons, 1991.

Contato

Prof. Dr. Vinícius Wasques

email: viniciuswasques@gmail.com

Departamento de Matemática

site: `https://viniciuswasques.github.io/home/`