Congruência e Equações Diofantinas Lineares

Edson Roberto Abe

08 / novembro / 2021

Congruência a módulo m

Definição: Dados a, b, m > 0 inteiros, diz-se que a é côngruo a b módulo m, denotado por:

$a \equiv b$ (mód. m) quando $m \mid (a - b)$, isto é, existe k que pertence a Z(inteiros) tal que $a - b = k.m$

Propriedades

i) $a \equiv b$ (mód. m) e $b \equiv c$ (mód. m) => $a \equiv c$ (mód. m)

ii) $a \equiv b$ (mód. m) e $c \equiv d$ (mód. m), então:

$a + c \equiv b + d$ (mód. m)

$a - c \equiv b - d$ (mód. m)

$a . c \equiv b . d$ (mód. m)

$a^n \equiv b^n$ (mód. m)

iii) $a \equiv b$ (mód. m), então:

$a + c \equiv b + c$ (mód. m)

$a . c \equiv b . c$ (mód. m)

1 – Prove que $30^{99} + 61^{100}$ é divisível por 31.

2 – Mostre que 41 divide $2^{20} - 1$.

3 – Prove que $2222^{5555} + 5555^{2222}$ é divisível por 7.

4 – Provar que $1979^{1980} + 64$ não é primo.

5 (BMO – 2000) – Mostre que, para cada inteiro positivo n, $121^n - 25^n + 1900^n - (-4)^n$ é divisível por 2000.

6 – Encontre os três últimos dígitos de 7^{9999}.

7 – Encontre os três últimos dígitos de 13^{398}, sabendo-se que $13^{400} \equiv 1$ (mód. 1000).

Pequeno Teorema de Fermat

Seja a um inteiro positivo e p um primo. Então $a^p \equiv a$ (mód. p).

8 – Prove que $20^{15} - 1$ é divisível por 11.31.61.

9 – Prove que $2^{70} + 3^{70}$ é divisível por 13.

10 – Prove que $2^{2021} + 6^{2021} + 1$ é divisível por 19.

Equações Diofantinas Lineares

Mdc(1172,144) = ?

Algoritmo de Euclides

Q	8	7	5
1172	144	20	**4 (mdc)**
R	20	4	**0**

1172 = 8.144 + 20 => **20** = **1172** – 8.**144**

144 = 7.20 + 4 => **4** = 144 – 7.20 = 144 – 7.(1172 – 8.144) = 57.**144** – 7.**1172**

Teorema: A congruência linear $a.x \equiv b$ (mód. m) tem solução se e somente se d divide b, sendo d = mdc(a,m).

11 – Resolver a equação 48x + 7y = 17.

12 – Resolver a equação 11x + 317y = 2.

13 – Em Marth, existem apenas notas de 3 e 7 marthreais. De quantos modos distintos podemos pagar uma conta de 246 marthreais usando as notas deste planeta?