CONGRUÊNCIAS

Yuri Gomes Lima, Fortaleza – CE

♦ Nível 1

INTRODUÇÃO

Aprenderemos aqui a utilizar Congruências para a resolução de vários problemas, como a solução de equações, a determinação de restos de divisões impossíveis de se fazer no "braço" e problemas de invariância (problemas onde algo, por exemplo a paridade, nunca muda).

Tal idéia foi desenvolvida por Gauss em um trabalho publicado em 1801 (*Disquisitiones Arithmeticae*), quando ele tinha apenas 24 anos de idade.

Aqui, trabalharemos sempre com os números naturais $IN = \{1,2,3,4,...\}$ e os números inteiros $Z = \{...,-2,-1,0,1,2,...\}$.

1. Divisibilidade

Definição: Sejam *a, b* inteiros. Dizemos que *a* divide *b* (notação: *a*| *b*) se existir um inteiro *c* tal que $b = ac$.

Em outras palavras, dizer que *a* divide *b* significa dizer que a divisão de *b* por *a* dá exata, ou que o resto dessa divisão é zero. Relembrando a divisão entre dois números, temos (Algoritmo da Divisão ou de Euclides):

b | a		No nosso caso: b | a
q → quociente			c
r → resto		0	
$(b = aq + r)$		$(b = ac)$	

Exemplos: 3 divide 12, pois $12 = 3x4$; 7 divide 56, pois $56 = 7x8$.

2. Congruência

A idéia de congruência é a seguinte: quando nos deparamos com um problema que relacione divisões, potenciações, etc., por que não trabalhamos com os restos das divisões ao invés dos próprios números? Quer dizer, por que não nos esquecemos dos números e ficamos apenas com os restos? Uma vez que esses restos são menores do que os números, é de se esperar que isso simplifique a solução desses problemas, o que de fato ocorre! Antes das aplicações, vamos ver um pouco de teoria.

Definição: Se *a,b e m* são inteiros (*m* > 0), dizemos que *a* é congruente a *b* módulo *m* se $m \mid (b-a)$. Denotaremos essa situação por $a \equiv b (\mathrm{mod}\, m)$.

Dizer que *a* é congruente a *b* módulo *m* significa que *a* e *b* deixam o mesmo resto quando divididos por *m*.

Exemplos: $21 \equiv 15 (\mathrm{mod}\, 6)$, pois $6 \mid (21-15)$. Observe que o resto da divisão dos dois números por 6 é igual a 5.

$4 \equiv 15 (\text{mod} 11)$, pois $11 | (4-15)$; $32 \equiv 0 (\text{mod}\, 4)$, pois $4 | (32-0)$.

Proposição 1: Sejam *a, b, c* e *m* inteiros, *m* > 0. Então:

(a) $a \equiv a (\text{mod}\, m)$;

(b) Se $a \equiv b (\text{mod}\, m)$, então $b \equiv a (\text{mod}\, m)$;

(c) Se $a \equiv b (\text{mod}\, m)$ e $b \equiv c (\text{mod}\, m)$, então $a \equiv c (\text{mod}\, m)$.

Demonstração:

(a) Como $m | 0 = (a-a)$, decorre que $a \equiv a (\text{mod}\, m)$.

(b) Se $a \equiv b (\text{mod}\, m)$, então $m | (b-a)$. Mas então $m | (a-b) \Rightarrow b \equiv a (\text{mod}\, m)$.

(c) Vamos utilizar o seguinte fato: se *m* divide dois números *X* e *Y*, então *m* divide a soma *X + Y* desses dois números. De fato, temos o seguinte:

$$\begin{cases} a \equiv b (\text{mod}\, m) \Rightarrow m | (b-a) \\ b \equiv c (\text{mod}\, m) \Rightarrow m | (c-b) \end{cases} \Rightarrow m | (b-a) + (c-b) = (c-a) \Rightarrow m | (c-a) \Rightarrow$$

$$\Rightarrow a \equiv c (\text{mod}\, m).$$

Você já deve estar percebendo que o símbolo ≡ (congruente) funciona de modo parecido ao símbolo = (igual), quer dizer, muitas das manipulações que fazemos com equações podem ser feitas com o sinal de congruência. Abaixo, estão outras dessas propriedades e os equivalentes a elas em equações.

Algumas propriedades úteis:

1) Se $a \equiv b (\text{mod}\, m)$, então $\begin{cases} a + c \equiv b + c (\text{mod}\, m) \\ a - c \equiv b - c (\text{mod}\, m) \\ ac \equiv bc (\text{mod}\, m) \end{cases}$, para todo inteiro *c*.

Em analogia com as equações, temos: se $a = b$, então $\begin{cases} a + c = b + c \\ a - c = b - c \\ ac = bc \end{cases}$

2) Se $a \equiv b (\text{mod}\, m)$ e $c \equiv d (\text{mod}\, m)$, então $\begin{cases} a + c \equiv b + d (\text{mod}\, m) \\ a - c \equiv b - d (\text{mod}\, m) \\ ac \equiv bd (\text{mod}\, m) \end{cases}$

Em analogia com as equações, temos: se $a = b$ e $c = d$, então $\begin{cases} a + c = b + d \\ a - c = b - d \\ ac = bd \end{cases}$

Como conseqüência da propriedade 2), temos que se $a \equiv a(\mathrm{mod}\, m)$, então $a.a \equiv b.b(\mathrm{mod}\, m) \Rightarrow a^2 \equiv b^2(\mathrm{mod}\, m)$. Daí, temos $a^2.a \equiv b^2.b(\mathrm{mod}\, m) \Rightarrow a^3 \equiv b^3(\mathrm{mod}\, m)$. Prosseguindo dessa forma, concluímos que $a^k \equiv b^k(\mathrm{mod}\, m)$, para todo natural *k*.

Uma propriedade que não vale é a de "cancelar" termos iguais. Nas equações, se tivermos por exemplo $6A = 6.5$, então podemos "cancelar" o 6, obtendo assim $A = 5$. Na congruência, isso não pode ser feito! De fato, se *A* for igual a 3, temos $6A \equiv 6.5(\mathrm{mod}\, 4)$, pois $4 \mid (6A - 6.5) = -12$, mas 3 não é igual a 5. (!!!)

Vamos agora aos exercícios (oba!).

Exercícios:

1. Mostre que o quadrado de um número inteiro não pode terminar em 2, 3, 7 ou 8.

2. A soma dos inteiros *a* e *b* termina por um zero. Mostre que os quadrados a^2 e b^2 terminam pelo mesmo algarismo.

3. Ache o resto da divisão de 4^{555} por 10.

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

5. **(OBM – 2003)** Seja $n = 9867$. Se você calculasse $n^3 - n^2$, você encontraria um número cujo algarismo das unidades é:

   A) 0 B) 2 C) 4 D) 6 E) 8

6. Mostre que os inteiros 3^n e 3^{n+4} terminam à direita pelo mesmo algarismo, qualquer que seja $n \in IN$.

7. A soma de dois quadrados ímpares pode ser um quadrado perfeito? Justifique.

8. Existe um inteiro positivo tal que seus fatores primos pertencem ao conjunto $\{2,3,5,7\}$ e que termina em 11? Se existir, ache o menor deles. Se não existir, mostre porquê.

9. Sabendo que *p* e $8p^2 + 1$ são primos, ache o valor de *p*.

10. Se *p* e $p^2 + 2$ são primos, mostre que $p^3 + 2$ também é um primo.

11. Mostre que não existem naturais *a*, *b* tais que $a^2 - 3b^2 = 8$.

12. **(Rússia)** Ache todos os pares de números primos *p*, *q* tais que $p^3 - q^5 = (p+q)^2$.

13. **(Hungria)** Em cada vértice de um quadrado há algumas fichas. Um movimento é escolher um vértice, tirar algumas fichas dele, escolher um vizinho e pôr o dobro de fichas retiradas

no vizinho. Se no início há 1, 0, 0, 0 fichas, é possível termos 1, 9, 8, 9 fichas em algum momento?

Fatos que ajudam nos Exercícios:

1) Congruência módulo 10 indica em qual algarismo o número termina. De fato, temos:
$17 \equiv 7 (\mathrm{mod}\, 10)$; $121 \equiv 1 (\mathrm{mod}\, 10)$; $523 \equiv 3 (\mathrm{mod}\, 10)$; $102 \equiv 2 (\mathrm{mod}\, 10)$.

2) A congruência módulo 2 nos dá a paridade do número:
(i) x é par $\Leftrightarrow x \equiv 0 (\mathrm{mod}\, 2)$;
(ii) x é ímpar $\Leftrightarrow x \equiv 1 (\mathrm{mod}\, 2)$.

3) Analisando um quadrado perfeito módulo 4, temos:
(i) $x \equiv 0 (\mathrm{mod}\, 4) \Rightarrow x^2 \equiv 0^2 (\mathrm{mod}\, 4) \Rightarrow x^2 \equiv 0 (\mathrm{mod}\, 4)$;
(ii) $x \equiv 1 (\mathrm{mod}\, 4) \Rightarrow x^2 \equiv 1^2 (\mathrm{mod}\, 4) \Rightarrow x^2 \equiv 1 (\mathrm{mod}\, 4)$;
(iii) $x \equiv 2 (\mathrm{mod}\, 4) \Rightarrow x^2 \equiv 2^2 \equiv 0 (\mathrm{mod}\, 4) \Rightarrow x^2 \equiv 0 (\mathrm{mod}\, 4)$;
(iv) $x \equiv 3 (\mathrm{mod}\, 4) \Rightarrow x^2 \equiv 3^2 \equiv 1 (\mathrm{mod}\, 4) \Rightarrow x^2 \equiv 1 (\mathrm{mod}\, 4)$.
Resumindo, se x é par, então $x^2 \equiv 0 (\mathrm{mod}\, 4)$, e se x é ímpar, então $x^2 \equiv 1 (\mathrm{mod}\, 4)$.

4) Analisando agora módulo 3, temos:
(i) $x \equiv 0 (\mathrm{mod}\, 3) \Rightarrow x^2 \equiv 0^2 (\mathrm{mod}\, 3) \Rightarrow x^2 \equiv 0 (\mathrm{mod}\, 3)$;
(ii) $x \equiv 1 (\mathrm{mod}\, 3) \Rightarrow x^2 \equiv 1^2 (\mathrm{mod}\, 3) \Rightarrow x^2 \equiv 1 (\mathrm{mod}\, 3)$;
(iii) $x \equiv 2 (\mathrm{mod}\, 3) \Rightarrow x^2 \equiv 2^2 \equiv 1 (\mathrm{mod}\, 3) \Rightarrow x^2 \equiv 1 (\mathrm{mod}\, 3)$.
Logo, não existe um inteiro x tal que $x^2 \equiv 2 (\mathrm{mod}\, 3)$.

5) Se p é um número primo maior do que 3, então $p \equiv 1$ ou 5 (mod 6). De fato, se:
(i) $p \equiv 0 (\mathrm{mod}\, 6) \Rightarrow p = 6k \Rightarrow p$ é múltiplo de 6 $\Rightarrow p$ não é primo (absurdo!).
(ii) $p \equiv 2 (\mathrm{mod}\, 6) \Rightarrow p = 6k + 2 \Rightarrow p$ é um primo par maior do que 5 (absurdo!).
(iii) $p \equiv 3 (\mathrm{mod}\, 6) \Rightarrow p = 6k + 3 \Rightarrow p$ é primo múltiplo de 3 maior do que 3 (absurdo!).
(iv) $p \equiv 4 (\mathrm{mod}\, 6) \Rightarrow p = 6k + 4 \Rightarrow$ idem a *(i)*.