**Aritmética Modular**

Acontece, frequentemente, que preferirmos, em certas circunstâncias, ignorar os múltiplos de um dado número quando fazemos cálculos.

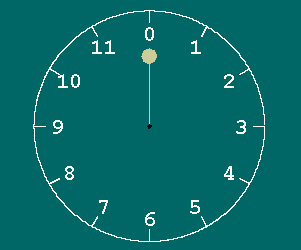
Pense nos dias da semana ou nas horas do dia; no primeiro caso ignoramos múltiplos de 7, no segundo, múltiplos de 24 (ou, muitas vezes, múltiplos de 12). São exemplos de "**aritmética módulo n**".

A "aritmética do relógio" é um exemplo de aritmética módulo n, neste caso n = 12. Se forem 7:00 horas e passarem 10 horas, então serão 5:00 horas (7 + 10 é igual a 5 módulo 12).

Se passarem 89 horas, serão 0:00 (7 + 89 é igual a 0 módulo 12).

Olhamos para o tempo entre os múltiplos de 12. A aritmética modular é a formalização matemática deste tipo de raciocínio.

Para ver se já percebeu a "aritmética do relógio", ou seja, as congruências módulo 12, veja o seguinte [relógio](http://www.atractor.pt/mat/alg_controlo/arit_modular/relogio_12.html):

[](http://www.atractor.pt/mat/alg_controlo/arit_modular/relogio_12.html)

<http://www.atractor.pt/mat/alg_controlo/arit_modular/mod_texto.htm>

**ARITMÉTICA MODULAR**

Quando estamos a utilizar a aritmética usual sobre os números naturais, apenas temos como números 1, 2, 3, 4, 5, ... Se em vez dos naturais considerarmos os números inteiros passamos a trabalhar com os números ..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...

**E no caso da Aritmética Modular?** Quais os números que se consideram nesta aritmética?

Vejamos o exemplo de **20 ≡ 8 (mod 12)**

Neste caso temos que o número 20 é identificado com o número 8, ou seja, temos que o número 20 ou o número 8 é equivalente (ou congruente) na Aritmética Módulo 12. Equivalente a estes dois, temos ainda uma infinidade de outros números: o 32, o 44, o 56, ... A este conjunto de números

{ 8, 20, 32, 44, 56, 68, ... }

chamamos classe de equivalência módulo 12 e esta classe vai ser identificada pelo menor deles, ou seja, pelo 8.

De um modo análogo, temos ainda mais 11 classes de equivalência nesta aritmética módulo 12, representadas pelos números: 0, 1, 2, 3, 4, 5, 6, 7, 9, 10, 11.

E estes vão ser os nossos "números" nesta aritmética: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 e 11.

Generalizando, os "números" considerados na Aritmética Modular módulo n são: 0, 1, 2, ..., n-2 e n-1.

Uma vez que este tipo de aritméticas apenas considera um número finito de "números", também se diz que a Aritmética Modular é uma aritmética finita.

Agora que já temos os nossos números, o passo seguinte é estudar as operações que se podem efetuar com estes números, em particular, a [adição](http://www.atractor.pt/mat/alg_controlo/arit_modular/adicao/som.htm) e a [multiplicação](http://www.atractor.pt/mat/alg_controlo/arit_modular/multiplicacao/multip_texto%20.htm).

**ADIÇÃO MODULAR**  **(Aritmética modular)**

Qual o resultado da adição **5 + 10** na **Aritmética Módulo 12** ?  
  
Na aritmética usual seria igual 15, mas para respondermos corretamente à nossa pergunta temos que saber qual é o resto que 15 tem quando é dividido por 12. Uma vez que este resto é igual a 3, dizemos que:  
  
**5 + 12 = 3 mod 12**http://www.atractor.pt/mat/alg_controlo/arit_modular/adicao/graphics/som__1%20copy.gif http://www.atractor.pt/mat/alg_controlo/arit_modular/adicao/graphics/som__1%20copy.gifhttp://www.atractor.pt/mat/alg_controlo/arit_modular/adicao/graphics/som__2%20copy.gifhttp://www.atractor.pt/mat/alg_controlo/arit_modular/adicao/graphics/som__2%20copy.gif

**9 + 6 = 3 mod 12**E se considerássemos agora o módulo 9 em vez de 12? Procedíamos de maneira análoga, mas neste caso a divisão considerada seria por 9 e não por 12. Uma vez que 15 = 1 x 9 + 6, dizemos que

**5 + 10 = 6 mod 9**

**MULTIPLICAÇÃO MODULAR** **(Aritmética modular)**

O resultado da multiplicação 5 x 10 na Aritmética Módulo 12?

Na aritmética usual seria igual a 50, mas para respondermos corretamente à nossa pergunta temos que saber qual é o resto que 50 tem quando é dividido por 12. Uma vez que este resto é igual a 2, dizemos que

5 x 10 = 2 mod 12http://www.atractor.pt/mat/alg_controlo/arit_modular/multiplicacao/graphics/multip_texto%20__3%20copy.gif

E se considerássemos agora o módulo 9 em vez de 12? Procederíamos de maneira análoga, mas neste caso a divisão considerada seria por 9 e não por 12. Uma vez que 50 = 5 x 9 + 5, dizíamos que:

5 x 10 = 5 mod 9

Outro link interessante:  
  
<http://www.numaboa.com/index.php?option=com_content&view=article&id=171&Itemid=72>

**EXPONENCIAÇÃO MODULAR**

**A exponenciação é realizada pela multiplicação repetida, com na aritmética comum.**

**Para encontrar 11E7 (mod 13) podemos proceder da seguinte forma:  
  
11E2 = 121 ≡ 4 (mod 13) 11E4 = (11E2)E2 ≡ 4E2 ≡3 (mod 13)  
  
11E7 ≡ 11 x 4 x 3 ≡ 132 ≡ 2 (mod 13)**

Uma das ferramentas mais importantes na Teoria dos Números é a aritmética modular ou congruências.

**Congruência** é a relação entre dois números inteiros que, divididos por um terceiro, chamado módulo de congruência, deixam o mesmo resto.   
  
Por exemplo, 20 é congruente a 14 com relação a 6 pois,

20/6=3 restando 2 e 14/6=2 restando 2

Suponha que *a, b* e *m* sejam números inteiros diferentes de zero.   
Dizemos que **a é congruente de b módulo m,** se **m dividir a-b**.   
Escrevemos isto como: **a Image b (mod m)**

Exemplos: 20 Image 14 (mod 6) , 20 - 14 = 6 / 6 = 1 (resto = 0)  
 -1 Image 9 (mod 5) , -1 - (+9) = -1 -9 = -10 / 2 = -5 (resto = 0)

1100 Image 2 (mod 9) , 1100-2 = 1098 / 9 = 122 (resto = 0)

E, na aritmética modular, o quadrado de qualquer número ímpar é 1 modulo 8.

3E2 = 1 (mod 8) , pois 9 - 1 = 8 / 8 = 1

5E2 = 1 (mod 8) , pois 25 - 1 = 24 / 8 = 3

Encontramos congruências em todos os cantos.   
  
Por exemplo, os relógios trabalham com módulos 12 ou 24 para as horas e módulo 60 para os minutos e segundos.   
  
Calendários usam módulo 7 para os dias da semana e módulo 12 para os meses.   
  
Outros exemplos: **73 ≡ 4 mod 23**  **21 ≡ -9 mod 10**

A linguagem da congruência foi desenvolvida por **Karl Friedrich Gauss** no início do século XIX.

Aritmética modular é utilizada no **Acordo de Chaves de Diffie-Hellman** e no desenvolvimento do algoritmo de criptografia de chave pública **RSA**.