Congruências

1. Congruência módulo m

1.1. Definição

Dizemos que a é congruente a b módulo m e escrevemos $a \equiv b \pmod{m}$ se, e somente se, a e b deixam o mesmo resto na suas divisões euclidianas por m.

Em particular, se r é o resto da divisão de a por m, então $a \equiv r \pmod{m}$.

1.2. Propriedades Operacionais

Sejam $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

(1) $a + c \equiv b + d \pmod{m}$

(2) $a - c \equiv b - d \pmod{m}$

(3) $na \equiv nb \pmod{m}$ para todo n natural

(4) $ac \equiv bd \pmod{m}$

(5) $a^n \equiv b^n \pmod{m}$ para todo n natural

As propriedades operacionais nos dizem que a congruência módulo m funciona quase como igual, pois dá para somar, subtrair e multiplicar congruências. Porém ainda não podemos dividir.

Uma situação em que podemos dividir é quando "cancelamos":

(6) Se m é inteiro tal que $\text{mdc}(m; n) = 1$, $na \equiv nb \pmod{m} \iff a \equiv b \pmod{m}$

Mas atenção!! Isso só vale quando $\text{mdc}(m; n) = 1$!!

Vejamos como congruências são úteis:

Exemplo 1.1.

Calcule o resto da divisão de 2^{2002} por 101.

Resolução

Observe que quando falamos em resto da divisão por um número m podemos pensar em congruências mód m. Assim, vamos calcular 2^{2002} mód 101.

Temos que uma potência de 2 "próxima" de 101 é $2^7 = 128$. Temos

$$\begin{aligned} 2^7 \equiv 27 \pmod{101} &\implies 2^{14} \equiv 729 \equiv 22 \pmod{101} \\ &\implies 2^{28} \equiv 484 \equiv -21 \pmod{101} \\ &\implies 2^{56} \equiv 441 \equiv -64 \equiv -2^6 \pmod{101} \\ &\implies 2^{50} \equiv -1 \pmod{101} \end{aligned}$$

Que bom, encontramos $2^{50} \equiv -1 \pmod{101}$! Agora podemos elevar os dois lados a qualquer número inteiro positivo!! Como $2002 = 50 \cdot 40 + 2$, temos

$$2^{2002} = 2^{50 \cdot 40 + 2} = \left(2^{50}\right)^{40} \cdot 2^2 \equiv (-1)^{40} \cdot 2^2 \equiv 4 \pmod{101},$$

ou seja, $2^{2002} \equiv 4 \pmod{101}$. Logo o resto da divisão de 2^{2002} por 101 é 4.

Uma boa estratégia na hora de calcular uma potência a^n módulo m é procurar um expoente d tal que $a^n \equiv \pm 1 \pmod{m}$.

Exercícios

01. Determine o resto das divisões de

(a) 4^{1234} por 3

(b) 20^{100} por 17

(c) $2000 \cdot 2^{2000} - 1$ por 3

02. Encontre o resto da divisão de 5^{20} por 26.

03. Mostre que $\left(835^5 + 6\right)^{18} - 1$ é divisível por 112.

04. Mostre que

(a) $2^{70} + 3^{70}$ é divisível por 13

(b) $2222^{5555} + 5555^{2222}$ é divisível por 7

05. Em cada casa do tabuleiro de xadrez, há o número de grãos de trigo indicado, como mostra a figura. O cavalo de Bruno & Bernardo começa a se movimentar no tabuleiro, de acordo com as regras usuais, a partir de uma casa qualquer. Quando ele atinge uma casa, come todos os grãos nela existentes (mas ele não come os grãos da casa inicial). Quando ele deixa uma casa, nós recolocamos a mesma quantidade de grãos que nela existiam. Depois de um certo tempo, o cavalo de Bruno & Bernardo retorna à casa inicial e come os grãos nela existentes. Prove que o número de grãos que o cavalo de Bruno & Bernardo comeu durante sua viagem é divisível por 3.

2^{63}	2^{62}	2^{61}	$\ldots$				
2^{16}	2^{17}	2^{18}	$\ldots$				
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8
2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7

06. Encontre os dois últimos dígitos de

(a) 7^{100}

(b) 2^{2000}

(c) $5^{600} + 19^{200}$

(d) $7^{2000} \times 2^{300}$

07. (a) Mostre que $81 \mid \underbrace{99\ldots9}_{\text{nove noves}}$.

(b) Determine o menor número da forma $99\ldots9$ que é divisível por 17.

08. Prove que, para todo n natural, $37^{n+2} + 16^{n+1} + 23^n$ é divisível por 7.

09. Mostre que, para todo n natural, $72^{2n+2} - 47^{2n} + 28^{2n-1}$ é divisível por 25.

10. Mostre que, para todos k, m, n naturais, $5^{5k+1} + 4^{5m+2} + 3^{5n}$ é divisível por 11.

11. Mostre que

(a) $2^{15} - 1$ e $2^{10} + 1$ são primos entre si.

(b) $2^{32} + 1$ e $2^4 + 1$ são primos entre si.

12. Mostre que 41 divide $11\ldots1$ (onde há $5k$ dígitos 1, k inteiro positivo).

13. Mostre que 91 divide $11\ldots1$ (onde há $6k$ dígitos 1, k inteiro positivo).

2. Usando congruências para resolver equações com números inteiros

As congruências ajudam bastante também na hora de resolvermos equações em inteiros (chamamos tais equações de *diofantinas*).

Exemplo 2.1.

Encontre todos os números naturais x e y tais que $2^x = 3^y - 1$.

Resolução

A primeira dúvida que poderia surgir é "que módulo vamos usar?" Lembra que uma estratégia era obter algo congruente a ± 1? Aqui não é diferente. Podemos, por exemplo, ver a congruência módulo 4, que é pertinho de 3 e é uma potência de 2:

$$2^x = 3^y - 1 \implies 2^x \equiv 3^y - 1 \pmod 4 \iff 2^x \equiv (-1)^y - 1 \pmod 4$$

Se $x = 0$, temos $2^0 = 3^y - 1 \iff 3^y = 2$, o que não é possível. Se $x = 1$, temos $2^1 = 3^y - 1 \iff 3^y = 3 \iff y = 1$, logo $x = 1$ e $y = 1$ é uma solução.

Se $x \geq 2$, temos $2^x \equiv 0 \pmod 4$. Logo devemos ter $(-1)^y - 1 \equiv 0 \pmod 4$, o que ocorre se, e somente se, y é par. Assim, $y = 2a$, onde a é natural e temos

$$2^x = 3^{2a} - 1 \iff 2^x = (3^a - 1)(3^a + 1)$$

Como $3^a - 1$ e $3^a + 1$ são divisores de uma potência de 2, então $3^a - 1$ e $3^a + 1$ são ambas potências de 2. Mas a diferença entre elas é $(3^a + 1) - (3^a - 1) = 2$, e as únicas potências de 2 tão "próximas" assim são 2 e 4. Conseqüentemente, $3^a - 1 = 2 \iff a = 1$ e logo $y = 2$ e $x = 3$. Enfim, as únicas soluções são $x = 3$ e $y = 2$ e $x = y = 1$.

Exercícios

14. Encontre todos os pares de inteiros positivos $(x; y)$ tais que $2^x = 1 + 3^y$.

15. Encontre todos os inteiros positivos x e y tais que $3^x - 2^y = 7$.

3. Referências Bibliográficas

- *Mathematical Olympiad Challenges*, Titu Andreescu e Răzvan Gelca.
- *Equations and Inequalities – Elementary Problems and Theorems in Algebra and Number Theory*, Jiří Herman, Radan Kučera e Jaromír Šimša.
- *Divisibilidade, Congruências e Aritmética Módulo n*, Carlos Gustavo Tamm Moreira (artigo da Revista Eureka! 2)