5. CONGRUÊNCIAS

Dizemos que $a \equiv b \pmod{m}$ (lê-se "a é congruente com b módulo m") se m dividir $a - b$.

Propriedades.

1. A congruência módulo m é uma relação de equivalência;
2. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$;
3. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$;
4. Se $a \equiv b \pmod{m}$ e $d|m$, então $a \equiv b \pmod{d}$;
5. Se $a \equiv b \pmod{m}$ e $c > 0$, então $ac \equiv bc \pmod{mc}$;

Nota. Em geral, a "lei do corte" não é válida!. Por exemplo, tem-se $2 \times 1 \equiv 2 \times 3 \pmod{4}$, mas $1 \not\equiv 3 \pmod{4}$;

6. Se $ac \equiv bc \pmod{m}$, então $a \equiv b \left(\mod \frac{m}{(m,c)}\right)$;

Teorema. *(Pequeno Teorema de Fermat) Seja p um número primo.*

1. *Se $p \nmid a$, então $a^{p-1} \equiv 1 \pmod{p}$.*
2. *$a^p \equiv a \pmod{p}$.*

Prova.

1. Consideremos os números a, $2a$, ..., $(p-1)a$. Nenhum destes números é múltiplo de p e não há dois que sejam congruentes módulo p. Logo os restos da divisão por p destes números são (não necessariamente por esta ordem) 1, 2, ..., $p - 1$. Então

$$a \times 2a \times \ldots \times (p-1)a \equiv 1 \times 2 \times (p-1) \pmod{p},$$

e portanto

$$a^{p-1}(1 \times 2 \times \ldots \times (p-1)) \equiv 1 \times 2 \times (p-1) \pmod{p}.$$

Como $\mathrm{mdc}(p, 1 \times 2 \times \ldots \times (p-1)) = 1$, a propriedade vi. mostra-nos que $a^{p-1} \equiv 1 \pmod{p}$.

2. Se $p \nmid a$, esta é uma consequência imediata da alínea anterior; se $p|a$, então $a^p \equiv a \equiv 0; \pmod{p}$.

6. CRITÉRIOS DE DIVISIBILIDADE

Um critério de divisibilidade é um método expedito de descobrir se um dado número é múltiplo de outro. Por exemplo, não é necessário efectuar a divisão de 253453485374858 e 349857934750345601 por 2 para saber que o primeiro é múltiplo de 2 e o segundo não é.

Critérios de divisibilidade por

2 Um número é par se e só se o seu algarismo das unidades for par.

Prova. Se o algarismo das unidades de n é a, então n pode escrever-se na forma $n = 10b + a$. Como $10 \equiv 0 \pmod 2$, então

$$n \text{ é par} \Leftrightarrow n \equiv 0 \pmod 2 \Leftrightarrow 10b + a \equiv 0 \pmod 2 \Leftrightarrow a \equiv 0 \pmod 2 \Leftrightarrow a \text{ é par.}$$

5 Um número é múltiplo de 5 se e só se o seu algarismo das unidades for múltiplo de 5.

Prova. Seja $n = 10b + a$. Como $10 \equiv 0 \pmod 5$, então

$$n \equiv 0 \pmod 5 \Leftrightarrow 10b + a \equiv 0 \pmod 5 \Leftrightarrow a \equiv 0 \pmod 5.$$

4 Um número é múltiplo de 4 se e só se a soma do seu algarismo das unidades com o dobro do seu algarismo das dezenas for múltipla de 4.

Prova. Seja $n = 100c + 10b + a$. Como $100 \equiv 0 \pmod 4$ e $10 \equiv 2 \pmod 4$, então

$$n \equiv 0 \pmod 4 \Leftrightarrow 100c + 10b + a \equiv 0 \pmod 4 \Leftrightarrow 2b + a \equiv 0 \pmod 4.$$

3 Um número é múltiplo de 3 se e só se a soma do seus algarismos for múltipla de 3.

Prova. Seja $n = a_0 + 10a_1 + 100a_2 + \cdots + 10^k a_k$. Como $10^i \equiv 1^i \equiv 1 \pmod 3$, então

$$n \equiv 0 \pmod 3 \Leftrightarrow a_0+10a_1+100a_2+\cdots+10^k a_k \equiv 0 \pmod 3 \Leftrightarrow a_0+a_1+a_2+\cdots+a_k \equiv 0 \pmod 3.$$

9 Um número é múltiplo de 9 se e só se a soma do seus algarismos for múltipla de 9.

Prova. Seja $n = a_0 + 10a_1 + 100a_2 + \cdots + 10^k a_k$. Como $10^i \equiv 1^i \equiv 1 \pmod 9$, então

$$n \equiv 0 \pmod 9 \Leftrightarrow a_0+10a_1+100a_2+\cdots+10^k a_k \equiv 0 \pmod 9 \Leftrightarrow a_0+a_1+a_2+\cdots+a_k \equiv 0 \pmod 9.$$

Poder-se-ia encontrar um critério de divisibilidade por 6, mas para ver se um número é múltiplo de 6, basta ver se ele é simultaneamente múltiplo de 2 e de 3.

7. EQUAÇÕES

Nesta secção vamos ver como resolver equações lineares envolvendo congruências.

Teorema.

1. Se $(a, m) = 1$, então a equação $ax \equiv b \pmod{m}$ tem uma única solução módulo m.
2. Se $(a, m) = d$, então a equação $ax \equiv b \pmod{m}$ tem d soluções módulo m se $d|b$ e nenhuma em caso contrário.

Teorema. *(Teorema Chinês dos Resíduos) Sejam $m_1, \ldots m_k$ números primos dois a dois. Então o sistema*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

tem uma única solução módulo $M = m_1 \times m_2 \times \cdots \times m_k$.

Prova. Apenas vamos mostrar a existência de uma solução do sistema, exibindo-a.

Sejam $n_1 = M/m_1, \ldots, n_k = M/M_k$.

A equação $n_i x \equiv 1 \pmod{m_i}$ tem uma única solução módulo m_i, para cada i. Designemos esta solução por s_i.

Seja $x = n_1 s_1 a_1 + n_2 s_2 a_2 + \cdots + n_k s_k a_k$. Como $n_1 s_1 a_1 \equiv a_1 \pmod{m_1}$ e $n_2 s_2 a_2 \equiv \cdots \equiv n_k s_k a_k \equiv 0 \pmod{m_i}$, então $x \equiv a_1 \pmod{m_1}$. Do mesmo modo se mostra que x é solução das restantes equações do sistema.