Aula 11. Congruências

Numa carta de 1640 dirigida a Bernhard Frénicle de Bessy, Fermat anunciava um resultado surpreendente: se p é um primo e a um inteiro que não é divisível por p, então p divide $a^{p-1} - 1$. Na mesma carta, comentava: "Eu lhe enviaria a demonstração se não temesse que ela é demasiado comprida".

A primeira demonstração desse resultado, conhecido como "Pequeno Teorema de Fermat" (para distingui-lo do Grande Teorema de Fermat, mencionado na Aula 8), foi publicada em 1736, quase um século depois, por Euler. Posteriormente, Euler deu outras demonstrações do mesmo resultado. Numa delas, ele utiliza frequentemente os "restos de divisões por p", que deram origem à Teoria das Congruências. Esse método de trabalho também foi usado por Lagrange e Legendre, mas só se tornou explícito nas Disquisitiones de Gauss, na qual aparecem a definição precisa e o simbolismo que se usa até hoje.

Veremos nos exemplos como a introdução dessa notação sintética simplifica o estudo de muitas questões de divisibilidade.

Definição

Seja n um inteiro positivo. Dois inteiros a, b chamam-se *congruentes modulo* n se n divide $(a - b)$. Neste caso escrevemos

$$a \equiv b \pmod{n}.$$

Exemplo 11.1

Por exemplo, temos

$$3 \equiv 24 (\text{mod } 21), \text{ pois } \quad 21 \mid (3 - 24),$$
$$3 \not\equiv 2 (\text{mod } 4), \text{ pois } \quad 4 \nmid (3 - 2).$$

Observação 11.1

Temos que

$$a \equiv b \pmod{2} \iff a, \text{ e } b \text{ tem a mesma paridade.}$$

Seja $a \in \mathbb{Z}$ e n inteiro positivo, usando Algoritmo da Divisão

temos

$$a = q \cdot n + r, \quad 0 \leq r < n.$$

Portanto, temos que

$$a \equiv r (\text{mod } n).$$

Observem que existem apenas n opções para r

$$r : 0, 1, 2, 3, \ldots, n-1$$

Portando qualquer inteiro a é congruente um e apenas um inteiro entre 0 e $n-1$.

Teorema 11.1

$$a \equiv b \pmod{n} \iff \begin{array}{l} a, b \text{ tem o mesmo} \\ \text{resto quando duvide} \\ \text{por } n. \end{array}$$

Prova

$[\Longrightarrow]$ Seja $a \equiv b \pmod{n}$. Assim $n \mid a - b$, logo $a - b = k \cdot n$. Aplicando Algoritmo da divisão de b por n, temos

$$b = q \cdot n + r, \quad 0 \leqslant r < n$$

Assim

$$\begin{aligned} & k \cdot n = a - b = a - q \cdot n + r \\ & \Rightarrow a = (k + q) \cdot n + r \\ & \Rightarrow a, b \quad \text{tem o mesmo resto quando divide por } n. \end{aligned}$$

$[\Longleftarrow]$ Se

$$\begin{aligned} a &= q_1 \cdot n + r \\ b &= q_2 \cdot n + r, \end{aligned}$$

Assim

$$a - b = (q_1 - q_2) \cdot n,$$

ou seja

$$a \equiv b \pmod{n}.$$

Exemplo 11.2

a) Se $a = 4 \cdot 3 + 1$ e $b = (-7) \cdot 3 + 1$, assim a, b temo o mesmo resto da divisão por 3, logo

$$a \equiv b \pmod{3}.$$

b) Por outro lado se, por exemplo $13 \equiv 6 (\text{mod} 7)$, assim $13, 6$ tem o mesmo resto da divisão por 7.

c) Se $2^5 \equiv 2 (\text{mod} 30)$ assim 2^5 tem o resto 2 quando dividimos por 30.

11.1 Propriedades

Teorema 11.2

Sejam: $n > 0$ um inteiro fixo e $a, b, c, d \in \mathbb{Z}$ qualquer inteiros. Assim

a) $a \equiv a \pmod{n}$.

b) Se $a \equiv b \pmod{n}$ assim $b \equiv a \pmod{n}$.

c) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, assim

$$a \equiv c \pmod{n}.$$

d) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ assim

$$\begin{aligned} a + c &\equiv b + d \pmod{n} \\ a \cdot c &\equiv b \cdot d \pmod{n}. \end{aligned}$$

e) Se $a \equiv b \pmod{n}$, assim

$$\begin{aligned} a + c &\equiv b + c \pmod{n} \\ a \cdot c &\equiv b \cdot c \pmod{n}, \end{aligned}$$

para qualquer inteiro c.

f) Se $a = b \pmod{n}$ assim

$$a^k = b^k \pmod{n},$$

para todo inteiro positivo k.

Prova

a) Como $n \mid 0 = (a - a)$, assim $a \equiv a \pmod{n}$.

b) Se $a \equiv b \pmod{n}$, assim $n \mid (a - b)$, logo $n \mid -(a - b) = b - a$ também. Portanto $b \equiv a \pmod{n}$.

c) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, assim $a - b = n \cdot q_1$ e $b - c = n \cdot q_2$. Somando estes igualdades temos $a - c = n \cdot (q_1 + q_2)$, logo $a \equiv c \pmod{n}$.

d) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, assim

$$\begin{aligned} a - b &= n \cdot q_1, \\ c - d &= n \cdot q_2, \end{aligned}$$

portanto $(a + b) - (b + d) = n \cdot (q_1 + q_2)$, logo

$$a + c \equiv b + d \pmod{n}$$

Prova

Alem disso temos que

$$a = b + n \cdot q_1,$$
$$c = d + n \cdot q_2,$$

portanto

$$\begin{aligned} a \cdot c &= (b + nq_1) \cdot (d + nq_2) \\ &= b \cdot d + nq_1 c + nq_2 b + n^2 q_1 q_2 \\ &= b \cdot d + n \cdot Q, \end{aligned}$$

logo

$$ac \equiv bd \pmod{n}.$$

e) temos

$$a \equiv b \pmod{n},$$
$$c \equiv c \pmod{n},$$

assim aplicando item d) para estes congruências, temos

$$a + c \equiv b + c \pmod{n},$$
$$ac \equiv bc \pmod{n}.$$

f) Vamos fazer a prova por indução. **Base** $\boxed{\text{k=1}}$

$$a \equiv b \pmod{n},$$

pelo condição.
Hipótese. Suponha que

$$a^k \equiv b^k \pmod{n},$$

Passo. Temos que

$$a^k \equiv b^k \pmod{n},$$
$$a \equiv b \pmod{n},$$

assim aplicando item d) temos

$$a^{k+1} \equiv b^{k+1} \pmod{n}.$$

Logo a formula vale para todos k.

11.2 Exemplos

Exemplo 11.3

Vamos determinar o resto da divisão de 5^{60} por 26. Escrevendo

$$5^{60} = 26q + r,$$

o problema equivale a determinar o inteiro r tal que $0 \leq r \leq 25$ e tal que

$$5^{60} \equiv r \pmod{26}.$$

Notamos que $5^2 = 25$, isto é, $5^2 \equiv -1 \pmod{26}$. Usando a parte (f) das propriedades, temos que

$$5^4 \equiv (-1)^2 \pmod{26},$$

isto é $5^{-4} \equiv 1 \pmod{26}$. Finalmente, $5^{60} = \left(5^4\right)^{15}$, logo

$$5^{60} \equiv (1)^{15} \pmod{26},$$

donde o resto da divisão de 5^{60} por 26 é 1.

Exemplo 11.4

Vamos provar que $41 \mid (2^{20} - 1)$. o problema equivale mostrar que

$$2^{20} \equiv 1 \pmod{41}.$$

Notamos que

$$2^{20} = (2^5)^4 = 32^4,$$

e que $32 \equiv -9 \pmod{41}$, isto é, $2^{20} \equiv (-9)^4 \pmod{26}$, usando a parte (f) das propriedades. Agora $(-9)^4 = 81^2$, e notamos que $81 \equiv -1 \pmod{41}$. Assim $81^2 \equiv 1 \pmod{41}$. Logo

$$81^{20} \equiv (-9)^4 = 81^2 \equiv 1 \pmod{41}.$$

Assim $41 \mid (2^{20} - 1)$.

Exemplo 11.5

Vamos provar que $41 \mid (2^{20} - 1)$. o problema equivale mostrar que

$$2^{20} \equiv 1 \pmod{41}.$$

Notamos que

$$2^{20} = (2^5)^4 = 32^4,$$

e que $32 \equiv -9 \pmod{41}$, isto é, $2^{20} \equiv (-9)^4 \pmod{26}$, usando a parte (f) das propriedades. Agora $(-9)^4 = 81^2$, e notamos que $81 \equiv -1 \pmod{41}$. Assim $81^2 \equiv 1 \pmod{41}$. Logo

$$81^{20} \equiv (-9)^4 = 81^2 \equiv 1 \pmod{41}.$$

Assim $41 \mid (2^{20} - 1)$.

Exemplo 11.6

Vamos provar encontrar o resto da divisão de

$$1! + 2! + 3! + \cdots + 100!$$

por 12. Notamos que $4! = 24 = 2 \cdot 12$, assim

$$4! \equiv 0 \pmod{12}$$

Semelhante

$$\begin{aligned} 5! = 4! \cdot 5 &\equiv 0 \cdot 5 = 0 \pmod{12} \\ 6! = 5! \cdot 6 &\equiv 0 \cdot 6 = 0 \pmod{12} \\ &\cdots \\ 100! = 5! \cdot 6 &\equiv 0 \cdot 6 = 0 \pmod{12} \end{aligned}$$

Assim, somando, temos

$$\begin{aligned} 1! + 2! + 3! + \cdots + 100! &\equiv 1! + 2! + 3! + 0 + 0 + \cdots + 0 \\ &\equiv 9 \pmod{12}. \end{aligned}$$

Logo o resto é 9.

11.3 *Cancelamento em congruências*

A propriedade e) diz que $a \equiv b \pmod{n}$ implique que $ac \equiv bc \pmod{n}$ para todo c. A reciproca não vale em geral. Por exemplo

$$2 \cdot 3 \equiv 2 \cdot 1 \pmod{4}$$

mas

$$3 \not\equiv 1 \pmod{4}.$$

Para cancelar o múltiplo comum podemos usa o seguinte Teorema

Teorema 11.3

Se $a \cdot c \equiv b \cdot c \pmod{n}$ assim

$$a \equiv b \pmod{n/d},$$

onde $d = \text{mdc}(c, n)$.

Prova

Temos que

$$c(a-b) = n \cdot q, \tag{11.1}$$

para algum q. Como $d = \text{mdc}(c,n)$ assim existem r,s com $\text{mdc}(r,s) = 1$ tal que

$$c = dr, \quad n = ds.$$

Loso $s = d/s$. Alem disso Equação (11.1) implique que

$$dr(a-b) = dsq,$$

ou seja

$$r(a-b) = sq.$$

Assim $s \mid r(a-b)$ e como $\text{mdc}(r,s) = 1$ podemos cancelar r pelo Lema de Euclides, logo $s \mid (a-b)$, ou seja

$$a \equiv b \pmod{s}.$$

O Teorema implique imediatamente os seguintes Corolários.

Corolário 11.1

Se $a \cdot c \equiv b \cdot c \pmod{n}$ e $\text{mdc}(c,n) = 1$, assim

$$a \equiv b \pmod{n}.$$

Corolário 11.2

Se $a \cdot c \equiv b \cdot c \pmod{p}$ com p um primo que não divide c assim

$$a \equiv b \pmod{p}.$$

Exercício 11.1: (Trabalho p/ casa)

Determine o algarismo das unidades de 3^{100}.
Resposta: 1.

Exercício 11.2: (Trabalho p/ casa)

Determinar o resto de divisão de 2^{50} por 7.
Resposta: 4.