Cheat Sheet: FMC - Unidade 2

Mateus Dias
Tecnologia da Informação - IMD/UFRN

23 de outubro de 2025

DEFINIÇÃO 0 - Divisores e Múltiplos

Essa definição não faz, realmente, parte do conteúdo, mas é fundamental para o entendimento de todas as próximas definições.

Parte 1 - Divisores

Um número inteiro d é divisor de um número inteiro a se, e somente se, ao dividir a por d, o resto for **zero**, ou seja, a divisão é exata.
Por exemplo, para o número 24 temos 8 divisores. São eles:

$$D = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

Parte 2 - Múltiplos

Um número inteiro b é múltiplo de um número inteiro a se, e somente se, existe um número inteiro k tal que:

$$b = ak$$

Por exemplo, se $a = 3$, os múltiplos de 3 são:

- Se $k = 2$, $b = 3 \cdot 2 = 6$
- Se $k = 5$, $b = 3 \cdot 5 = 15$

O conjunto dos múltiplos de 3 é:

$$M(3) = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$$

Parte 3 - Relação entre Divisores e Múltiplos

Se b é um **múltiplo** de a, isso significa que a é um **divisor** de b. Esta relação será explorada melhor na definição de **divisibilidade**.

DEFINIÇÃO 1 - Divisibilidade

Sejam $a, b \in \mathbb{Z}$. Dizemos que a divide b se, e somente se $\exists k \in \mathbb{Z}$ tal que: $ak = b$.

$$a \mid b \iff (\exists k \in \mathbb{Z})(ak = b).$$

DEFINIÇÃO 2 - Módulo

Sejam $a, b, m \in \mathbb{Z}$. a é congruente a b módulo m se, e somente se $m \mid a - b$.

$$a \equiv b \pmod{m} \iff m \mid a - b$$

Também é possível usar o módulo para representar o resto de uma divisão. Pela definição de divisão euclidiana, sabe-se que um número arbitrário $D \in \mathbb{Z}$ pode ser representado como

$$D = dq + r.$$

Com **D** sendo o **dividendo**, **d** o **divisor**, **q** o **quociente** e **r** o **resto** $(0 \leq r < |d|)$.
Nesse sentido, podemos afirmar que:

$$D \bmod d = r.$$

TEOREMA 1

Sejam $a, b, m \in \mathbb{Z}$, com $m > 0$. a é congruente a b módulo m se, e somente se $a \bmod m = b \bmod m$.

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m.$$

Prova ($\implies$)

Suponha $a, b, m \in \mathbb{Z}$ tal que $a \equiv b \pmod{m}$.
Pelas definições 2 e 1, respectivamente, temos que:

$$\begin{aligned} &m \mid a - b \\ &mk = a - b \\ &a = b + mk \quad \textbf{(I)} \end{aligned}$$

Pela definição do resto, ao dividir b por m, temos:

$$b = q_b \cdot m + r_b \quad \textbf{(II)}$$

Onde $q_b \in \mathbb{Z}$ e $r_b = b \bmod m$, com $0 \leq r_b < m$.
Substituindo **(II)** em **(I)**:

$$a = (q_b \cdot m + r_b) + mk$$
$$a = mq_b + mk + r_b$$
$$a = m \cdot (q_b + k) + r_b$$

Tome $q_a = q_b + k$. Como $q_a \in \mathbb{Z}$ e $0 \leq r_b < m$, podemos dizer que r_b é o resto da divisão de a por m, isto é, $a \bmod m = r_b$.
Como $r_b = b \bmod m$, temos que:

$$a \bmod m = b \bmod m.$$

Prova ($\Longleftarrow$)

Suponha $a, b, m \in \mathbb{Z}$ tal que $a \bmod m = b \bmod m$. Seja r o valor comum do resto, de forma que:

$$r = a \bmod m = b \bmod m$$

Pela definição do resto, podemos escrever a e b como:

$$a = q_a \cdot m + r$$
$$b = q_b \cdot m + r$$

Onde $q_a, q_b \in \mathbb{Z}$ e $0 \leq r < m$. Dessa forma, a diferença $a - b$ fica desta forma:

$$a - b = (q_a \cdot m + r) - (q_b \cdot m + r)$$
$$a - b = q_a \cdot m + r - q_b \cdot m - r$$
$$a - b = m \cdot (q_a - q_b)$$

Seja $k = q_a - q_b$. Como $q_a \in \mathbb{Z}$ e $q_b \in \mathbb{Z}$ temos que $k \in \mathbb{Z}$. Portanto:

$$a - b = mk$$

Pela definição 1 e 2, respectivamente, temos que:

$$m \mid a - b$$
$$a \equiv b \pmod{m}$$

$\blacksquare$

DEFINIÇÃO 3 - Máximo Divisor Comum

Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. O MDC de a e b, denotado por $mdc(a, b)$ é o único inteiro positivo d que satisfaz as seguintes condições:

1. $d \mid a$
2. $d \mid b$
3. $\forall c \in \mathbb{Z}[((c \mid a) \wedge (c \mid b)) \implies c \mid d]$

Em outros termos, d é o maior número inteiro positivo que divide a e b ao mesmo tempo.

Exemplos

1. Calcular o $mdc(12, 18)$.

Divisores de 12: $\{1, 2, 3, 4, 6, 12\}$
Divisores de 18: $\{1, 2, 3, 6, 9, 18\}$
Divisores comuns: $\{1, 2, 3, 6\}$
Máximo Divisor Comum (MDC): 6

Algoritmo de Euclides

O algoritmo de Euclides é um método simples para encontrar o MDC entre dois números inteiros diferentes de zero. Ele é um derivado da divisão euclidiana:

$$D = dq + r.$$

Com **D** sendo o **dividendo**, **d** o **divisor**, **q** o **quociente** e **r** o **resto** $(0 \leq r < |d|)$.

Se queremos calcular $mdc(a, b)$, podemos assumir $D_1 = \max(a, b)$ como o dividendo inicial e $d_1 = \min(a, b)$ como o divisor inicial.

O algoritmo procede em etapas sucessivas, onde o resto de cada divisão se torna o novo divisor e o divisor anterior se torna o novo dividendo, até que $r_i = 0$ (onde i é o número de iterações). O último resto **não nulo** é o $mdc(a, b)$.

Exemplos

2. Calcular o $mdc(270, 192)$.

$$270 = 192 \cdot 1 + 78 \quad (1)$$
$$192 = 78 \cdot 2 + 36 \quad (2)$$
$$78 = 36 \cdot 2 + 6 \quad (3)$$
$$36 = 6 \cdot 6 + 0 \quad (4)$$

Portanto, o $\mathbf{mdc(270, 192)}$ é igual ao último resto não nulo, ou seja, **6**.

DEFINIÇÃO 4 - Mínimo Múltiplo Comum

Sejam $a, b \in \mathbb{Z}$. O $mmc(a, b)$ é o menor número inteiro positivo que é múltiplo de a e b simultaneamente.

Exemplos

1. Calcular o $mmc(4, 6)$.

$$\textbf{Múltiplos de 4: } \{4, 8, \mathbf{12}, 16, 20, 24, ...\}$$
$$\textbf{Múltiplos de 6: } \{6, \mathbf{12}, 18, 24, 30, 36, ...\}$$

O menor dos múltiplos comuns é 12, portanto $mmc(4, 6) = 12$.

Métodos para calcular o MMC

É possível conectar os conceitos de MMC e MDC com uma fórmula relacionada à Matemática Discreta:

$$mmc(a, b) = \frac{|a \cdot b|}{mdc(a, b)}$$

Este é o método que apresenta maior eficiência computacional para calcular o MMC entre dois números, mas também existe o método da fatoração prima (mais útil para calcular o MMC entre três ou mais números):

1. **Fatore** todos os números em seus fatores primos;
2. O **MMC** é o produto de todos os fatores primos distintos, cada um elevado à maior potência em que ele aparece em qualquer uma das fatorações.

Exemplos

2. Calcular o $mmc(12, 18)$ usando o primeiro método.

1. Calcular o **mdc(12,18)**:
   Segundo o método apresentado na **definição 3**:

$$18 = 12 \cdot 1 + 6 \tag{1}$$
$$12 = 6 \cdot 2 + 0 \tag{2}$$

   Portanto, $mdc(12, 18) = \mathbf{6}$.

2. Substituir na fórmula:

$$mmc(12,18) = \frac{|12 \cdot 18|}{6}$$

$$mmc(12,18) = \frac{216}{6}$$

$$mmc(12,18) = 36$$

3. Calcular o $mmc(12, 18)$ usando o segundo método.

1. Fatore 12 e 18 em seus respectivos fatores primos:

$$12 = 2^2 \cdot 3^1$$
$$18 = 2^1 \cdot 3^2$$

2. Fatores e maiores potências:
   - Fator 2: 2^2
   - Fator 3: 3^2

3. Cálculo:

$$mmc(12,18) = 2^2 \cdot 3^2$$
$$mmc(12,18) = 4 \cdot 9$$
$$mmc(12,18) = 36$$

O MMC entre a e b também pode ser interpretado como "o primeiro número em que a irá *se encontrar* com b quando ambos forem multiplicados por números naturais".

TEOREMA 2 - Teorema de Bézout

Sejam $a, b \in \mathbb{Z}$ com $a, b > 0$. O $mdc(a, b)$ pode ser escrito como uma combinação linear de a e b:

$$mdc(a, b) = sa + tb$$

Com $s, t \in \mathbb{Z}$.
O método para descobrir os valores de s e t é substituir consecutivamente os valores no algoritmo de Euclides.

Exemplos

1. Expressar o mdc(270,192) como uma combinação linear de 270 e 192.

$$
\begin{aligned}
&270 = 192 \cdot 1 + 78 \\
&192 = 78 \cdot 2 + 36 \\
&78 = 36 \cdot 2 + 6 \\
&36 = 6 \cdot 6 + 0 \\
\\
&6 = 78 - 2 \cdot 36 \\
&6 = 78 - 2 \cdot (192 - 2 \cdot 78) \\
&6 = (270 - 1 \cdot 192) - 2 \cdot (192 - 2 \cdot (270 - 1 \cdot 192)) \\
&6 = 270 - 1 \cdot 192 - 2 \cdot 192 + 4 \cdot 270 - 4 \cdot 192 \\
&6 = 5 \cdot 270 - 7 \cdot 192
\end{aligned}
$$

Portanto, $s = 5, t = -7$.

DEFINIÇÃO 5 - Inverso Multiplicativo Modular

Este é um conceito essencial que se relaciona com o conceito de congruência linear (**definição 6**).

Sejam $a, m \in \mathbb{Z}$. O inverso multiplicativo modular de a mod m é o inteiro x tal que:

$$ax \equiv 1 \pmod{m}$$

Condição de existência

O inverso multiplicativo modular de a mod m existe se, e somente se $mdc(a, m) = 1$, isto é, se a e m forem **coprimos** ou **primos entre si**.

Métodos para encontrar

É possível encontrar o inverso multiplicativo de a mod m facilmente usando o **teorema 2 - teorema de Bézout**.

Ao escrever o $mdc(a, m)$ como uma combinação linear de a e m, o coeficiente de a é o seu inverso multiplicativo.

Exemplos

1. Encontrar o inverso multiplicativo de 3 mod 7.

$$3x \equiv 1 \pmod 7$$

Primeiro, precisamos calcular $mdc(3, 7)$.

$$7 = 3 \cdot 2 + 1$$
$$3 = 1 \cdot 3 + 0$$

Como $mdc(3, 7) = 1$, o inverso multiplicativo existe.
Agora, escrevemos 1 como uma combinação linear de 3 e 7.

$$1 = 1 \cdot 7 - 2 \cdot 3$$

O coeficiente de 3 é -2, então $x = -2$.

Como o inverso multiplicativo encontrado é um número negativo, podemos fazer a operação $x \bmod m$ para encontrar um inverso multiplicativo positivo (o que é uma boa prática).

$$-2 \bmod 7 = 5$$

Logo, o inverso multiplicativo que procuramos é **5**.

Obs: Para encontrar um inverso multiplicativo positivo também é possível somar m a x até que x seja maior ou igual a 1.

DEFINIÇÃO 6 - Congruência Linear

Uma congruência linear é uma equação na forma $ax \equiv b \pmod m$. Uma congruência linear tem solução se, e somente se $mdc(a, m) \mid b$.

Para resolver a congruência linear, é necessário seguir os seguintes passos:

1. Encontrar o inverso multiplicativo de a – denotado por $\overline{a}$ ou a^{-1} – utilizando o método descrito na **definição 5**.

$$a\overline{a} \equiv 1 \pmod m$$

2. Multiplicar os dois lados da congruência por $\overline{a}$.

$$\overline{a}ax \equiv \overline{a}b \pmod{m}$$

3. Simplificando, o resultado fica:

$$x \equiv \overline{a}b \pmod{m}$$

4. Se $\overline{a}b < 1$ ou $\overline{a}b \geq m$, é necessário executar a operação ($\overline{a}b \bmod m$) para encontrar a menor congruência natural.

Exemplos

1. Calcular $17x \equiv 82 \pmod{11}$

$$17\overline{a} \equiv 1 \pmod{11}$$

$$\begin{aligned}
&17 = 11 \cdot 1 + 6 \\
&11 = 6 \cdot 1 + 5 \\
&6 = 5 \cdot 1 + 1
\end{aligned}$$

$$\begin{aligned}
&1 = 6 - 1 \cdot 5 \\
&1 = 6 - 1 \cdot (11 - 1 \cdot 6) \\
&1 = (17 - 1 \cdot 11) - 1 \cdot (11 - 1 \cdot (17 - 1 \cdot 11)) \\
&1 = 17 - 1 \cdot 11 - 1 \cdot 11 + 1 \cdot 17 - 1 \cdot 11 \\
&1 = 2 \cdot 17 - 3 \cdot 11
\end{aligned}$$

$$\overline{a} = 2$$

$$\begin{aligned}
&2 \cdot 17x \equiv 2 \cdot 82 \pmod{11} \\
&34x \equiv 164 \pmod{11} \\
&\boxed{x \equiv 10 \pmod{11}}
\end{aligned}$$

Também é possível escrever a solução na forma de um conjunto solução, usando as definições 2 e 1 **(módulo e divisibilidade)**, respectivamente:

$$\begin{aligned}
11 &\mid x - 10 \\
11k &= x - 10 \\
x &= 11k + 10
\end{aligned}$$

$$S = \{x \in \mathbb{Z} \mid x = 10 + 11k, k \in \mathbb{Z}\}$$

TEOREMA 3 - Teorema Chinês do Resto

O teorema chinês do resto é um teorema que pode ser usado para resolver sistemas de congruências lineares do tipo:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_{n-1} \pmod{m_{n-1}} \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Obs: A solução só existe se $mdc(m_i, m_j) = 1$ para todo $i \neq j$.

Algoritmo de solução

1. Calcular o módulo total (M):

$$M = m_1 \cdot m_2 \cdot \dots \cdot m_n$$

2. Calcular os M_i:

   M_i é o produto de todos os módulos do sistema, excluindo o módulo m_i.

3. Encontrar o inverso y_i:

$$M_i \cdot y_i \equiv 1 \pmod{m_i}$$

4. Calcular a solução (x):

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n \pmod{M}$$

   Obs: Na maioria das vezes, a solução final será o resto da divisão dessa soma por M.

Exemplos

1. Calcular a solução de:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

1. Módulo total (**M**):

$$M = 3 \cdot 5 \cdot 7$$
$$M = 105$$

2. Cálculo dos $\mathbf{M_i}$:

$$M_1 = 5 \cdot 7 = 35$$
$$M_2 = 3 \cdot 7 = 21$$
$$M_3 = 3 \cdot 5 = 15$$

3. Inverso $\mathbf{y_i}$:

$$
\begin{aligned}
35 \cdot y_1 &\equiv 1 \pmod{3}\\
21 \cdot y_2 &\equiv 1 \pmod{5}\\
15 \cdot y_3 &\equiv 1 \pmod{7}
\end{aligned}
$$

$$
\begin{aligned}
y_1 &= 2\\
y_2 &= 1\\
y_3 &= 1
\end{aligned}
$$

4. Solução $\mathbf{x}$:

$$
\begin{aligned}
&x \equiv (2 \cdot 35 \cdot 2) + (3 \cdot 21 \cdot 1) + (2 \cdot 15 \cdot 1) \pmod{105}\\
&x \equiv 140 + 63 + 30 \pmod{105}\\
&x \equiv 233 \pmod{105}
\end{aligned}
$$

$$\boxed{x \equiv 23 \pmod{105}}$$

TEOREMA 4 - Pequeno Teorema de Fermat

Este é um teorema desenvolvido pelo matemático francês Pierre de Fermat, e possibilita a simplificação de cálculos com potências grandes na aritmética modular.
O teorema pode ser enunciado de duas formas:

Primeira forma

Seja p um número primo e $a \in \mathbb{Z}$. Então:

$$a^p \equiv a \pmod{p}$$

Ou seja, se elevarmos a à potência do primo p e depois dividirmos o resultado por p, o resto é igual ao resto da divisão de a por p.

Segunda forma

Esta é a forma mais usada.
Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$ (ou seja, $mdc(a, p) = 1$). Então:

$$a^{p-1} \equiv 1 \pmod{p}$$

Ou seja, se elevarmos a à potência de $p - 1$ e depois dividirmos o resultado por p, o resultado vai sempre ser igual a 1.

Exemplos

1. Calcular 2^{23} mod 5 (ou seja, o resto da divisão de 2^{23} por 5).

Como 5 é um número primo e $5 \nmid 2$, é possível utilizar o pequeno teorema de Fermat.

$$
\begin{align}
2^{5-1} &\equiv 1 \pmod 5 \tag{1}\\
2^4 &\equiv 1 \pmod 5 \tag{2}\\
(2^4)^5 &\equiv 1^5 \pmod 5 \tag{3}\\
(2^4)^5 \cdot 2^3 &\equiv 1^5 \cdot 2^3 \pmod 5 \tag{4}\\
2^{23} &\equiv 8 \pmod 5 \tag{5}\\
2^{23} &\equiv 3 \pmod 5 \tag{6}
\end{align}
$$

Portanto, o resto da divisão de 2^{23} por 5 é igual a 3.

APLICAÇÃO 1 - Números Inteiros Grandes

Na área da computação, muitas vezes é necessário computar números inteiros grandes que, a princípio, não podem ser computados por um processador comum de computador.

Codificação

Sejam $m_1, m_2, \ldots, m_n$ inteiros maiores que 1 e primos entre si, com m sendo o produto entre eles e $a \in \mathbb{Z}$ tal que $0 \leq a < m$. É possível representar todos os números a como a n-upla:

$$a = (a \text{ mod } m_1, a \text{ mod } m_2, \ldots, a \text{ mod } m_n).$$

Por exemplo, se definirmos $m_1 = 3$, $m_2 = 5$, teremos as seguintes representações:

$0 = (0, 0)$	$5 = (2, 0)$	$10 = (1, 0)$
$1 = (1, 1)$	$6 = (0, 1)$	$11 = (2, 1)$
$2 = (2, 2)$	$7 = (1, 2)$	$12 = (0, 2)$
$3 = (0, 3)$	$8 = (2, 3)$	$13 = (1, 3)$
$4 = (1, 4)$	$9 = (0, 4)$	$14 = (2, 4)$

Decodificação

Dada uma n-upla e seus m_i, é possível chegar facilmente ao valor representado usando o **teorema chinês do resto** (teorema 3).

Como exemplo, podemos tentar descobrir o valor representado por uma dupla aleatória do exemplo de **codificação**. Vamos usar a dupla $(\mathbf{2}, \mathbf{1})$ e $m_1 = 3, m_2 = 5$:

$$x = (2, 1) = (x \bmod 3, x \bmod 5)$$

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \end{cases}$$

$$M = 3 \cdot 5 = 15$$

$$M_1 = 5$$
$$M_2 = 3$$

$$y_1 = 2$$
$$y_2 = 2$$

$$x \equiv (2 \cdot 5 \cdot 2) + (1 \cdot 3 \cdot 2) \pmod{15}$$
$$x \equiv 20 + 6 \pmod{15}$$
$$x \equiv 26 \pmod{15}$$
$$\boxed{x \equiv 11 \pmod{15}}$$

Obs: Nesse caso, podemos considerar como verdadeira apenas a primeira equivalência, portanto $x = 11$.

Operações aritméticas

Para realizar operações aritméticas com as n-uplas, basta realizar tal operação entre o i-ésimo termo da primeira n-upla com o seu respectivo na segunda n-upla, e com o resultado realizar a operação módulo com o m_i correspondente.

Restrições

Para realizar a operação, o valor resultante deve poder ser escrito também como uma n-upla. Portanto, o resultado deve ser um dos possíveis valores de a $(0 \leq a < m)$.

Exemplo

Sejam $a = 2, b = 3, m_1 = 3, m_2 = 5$.

$$a + b = 2 + 3 = (2, 2) + (0, 3)$$
$$a + b = ((2 + 0) \bmod 3, (2 + 3) \bmod 5)$$
$$a + b = (2 \bmod 3, 5 \bmod 5)$$
$$a + b = (2, 0)$$
$$a + b = 5$$

$$\begin{aligned}
a \cdot b &= 2 \cdot 3 = (2,2) \cdot (0,3) \\
a \cdot b &= ((2 \cdot 0) \bmod 3, (2 \cdot 3) \bmod 5) \\
a \cdot b &= (0 \bmod 3, 6 \bmod 5) \\
a \cdot b &= (0,1) \\
a \cdot b &= 6
\end{aligned}$$

NOTA: Aqui acabam os conteúdos da primeira prova da unidade 2 (que foi dividida em duas partes, sendo a primeira no dia **15 de outubro**).

DEFINIÇÃO 7 - Função de Euler

A função de Euler, função totiente ou função phi é fundamental para os próximos tópicos, especialmente o de criptografia de chave pública ou assimétrica.

Notação:

$$\phi(n)$$

Ela calcula a quantidade de números naturais não nulos m menores ou iguais a n tais que m e n são relativamente primos, ou seja, $mdc(m,n) = 1$

Exemplos

1. Calcular $\phi(6)$:

- Os números $m \leq 6$ são $\{1,2,3,4,5,6\}$.
  - $mdc(1,6) = 1$ **(coprimo)**
  - $mdc(2,6) = 2$ (não coprimo)
  - $mdc(3,6) = 3$ (não coprimo)
  - $mdc(4,6) = 2$ (não coprimo)
  - $mdc(5,6) = 1$ **(coprimo)**
  - $mdc(6,6) = 6$ (não coprimo)
- Os coprimos são **1** e **5**, então $\phi(6) = 2$.

2. Calcular $\phi(7)$:

- Como 7 é um número primo, todos os números naturais não nulos até $7 - 1$ são coprimos com ele, portanto $\phi(7) = 6$.

Principais fórmulas

Existem algumas fórmulas e propriedades que ajudam a calcular $\phi(n)$. Sejam $p, q, m, n \in \mathbb{Z}$ com $p \neq q$, p e q números primos e m e n coprimos.

$$\phi(p) = p - 1 \tag{1}$$
$$\phi(p \cdot q) = (p-1) \cdot (q-1) \tag{2}$$
$$\phi(p^2) = p \cdot (p-1) \tag{3}$$
$$\phi(m \cdot n) = \phi(m) \cdot \phi(n) \tag{4}$$

Exemplos

3. Calcular $\phi(19)$:

- Pela fórmula **(1)**, $\phi(7) = 7 - 1 = 6$.

4. Calcular $\phi(35)$:

- Decompondo 35 em fatores primos, obtemos $35 = 7 \cdot 5$.
- Pela fórmula **(2)**, $\phi(35) = \phi(7 \cdot 5) = (7-1) \cdot (5-1) = 6 \cdot 4 = 24$.

5. Calcular $\phi(49)$:

- Sabe-se que $49 = 7^2$.
- Pela fórmula **(3)**, $\phi(49) = \phi(7^2) = 7 \cdot (7-1) = 7 \cdot 6 = 42$.

TEOREMA 5 - Teorema de Euler

O teorema de Euler, também conhecido como teorema de Fermat-Euler, é uma generalização do Pequeno Teorema de Fermat **(teorema 4)**. Seu enunciado é o seguinte:

Sejam a e n dois inteiros positivos, onde $n > 1$. Se $mdc(a, n) = 1$, então:

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Exemplos

1. Calcular $7^{100} \bmod 10$.

- Como $mdc(7, 10) = 1$, a condição é satisfeita, portanto, $7^{\phi(10)} \equiv 1 \pmod{10}$.
- Agora precisamos calcular $\phi(10)$.

$$
\begin{aligned}
\phi(10) &= \phi(2 \cdot 5) \\
&= (2-1) \cdot (5-1) \\
&= 1 \cdot 4 \\
\phi(10) &= 4
\end{aligned}
$$

- Portanto, temos que $7^4 \equiv 1 \pmod{10}$. Agora, podemos simplificar a potência para calcular 7^{100}:

$$
\begin{aligned}
7^4 &\equiv 1 \pmod{10} \\
(7^4)^{25} &\equiv 1^{25} \pmod{10} \\
7^{100} &\equiv 1 \pmod{10}
\end{aligned}
$$