Universidade Federal do Rio Grande do Norte
Instituto Metrópole Digital
Bacharelado em Tecnologia da Informação
Disciplina: Fundamentos Matemáticos para Computação I (IMD0028)
Semestre: 2015.2
Professor: Patrick Cesar Alves Terrematte

— Avaliação: Unidade 2 —

Nome: _____ **Turma:** _____

- Todas as resoluções devem incluir os cálculos e raciocínios usados para obter a solução.
- No cabeçalho da folha de rascunho, escreva seu nome.
- No rodapé direito, confira a ordem das folhas, e escreva "Página n de m", para n e $m \in \mathbb{N}$.
- Se for o caso, consideraremos valores já calculados em outras questões, basta indicar e justificar.

1. Demonstre, ou refute:

(a) $\forall n \geq 1, n \in \mathbb{N},\ n^3 \equiv n \pmod 3$ **(_____/2,0 pts)**

Resposta:
Demonstração por casos. Verificar a congruência para os 3 únicos resíduos possíveis $r \in \{0, 1, 2\}$. Como qualquer número natural se reduz a um resíduo, os outros casos decorrem destes três casos:
Caso 1: $r = 0$. Note $0^3 \equiv 0 \pmod 3$, dado que $(0 \bmod 3) = (0 \bmod 3)$ pela definição de congruência.
Caso 2: $r = 1$. Note $1^3 \equiv 1 \pmod 3$, dado que $(1 \bmod 3) = (1 \bmod 3)$ pela definição de congruência.
Caso 3: $r = 2$. Note $2^3 \equiv 2 \pmod 3$, dado que $(8 \bmod 3) = (2 \bmod 3)$ pela definição de congruência.

Demonstração por indução simples alternativa.
Passo Base: Para n = 1, note que para $1^3 \equiv 1 \pmod 3$, temos que $1 \equiv 1 (\text{mod } 3)$.
Passo Indutivo:
Suponha um arbitrário $k \in \mathbb{N}$, tal que $k^3 \equiv k \pmod 3$. Logo, pela definição de equivalência modular, temos que $3 \mid (k^3 - k)$. Ou seja, pela definição de divisibilidade:
(HI) $\exists w_1 \in \mathbb{Z}, k^3 - k = 3w_1$
- Portanto, *temos que provar que* $\exists w_2 \in \mathbb{Z}, (k+1)^3 - (k+1) = 3w_2$

$$\begin{aligned}(k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - k - 1 \\ &= k^3 + 3k^2 + 3k - k \\ &= (k^3 - k) + 3k^2 + 3k \\ &= 3w_1 + 3k^2 + 3k, \text{ pela HI.} \\ &= 3(w_1 + k^2 + k) \\ &= 3w_2, \text{ onde } w_2 = w_1 + k^2 + k \text{ e } w_2 \in \mathbb{Z}\end{aligned}$$

Pela definição de congruência, temos que $(k+1)^3 \equiv (k+1) \pmod 3$. Portanto, é verdadeiro que $\forall n \geq 1, n \in N,\ n^3 \equiv n \pmod 3$.

(b) $\forall n \geq 1, n \in N,\ 9 \mid (4^n + 6n - 1)$. **(_____/2,0 pts)**

Note que uma hipótese pode ser utilizada mais de uma vez, ou podemos demonstrar lemas auxiliares.

Resposta:
Demonstração por indução simples.
Passo Base: Para n = 1, note que para $9 \mid (4^1 + 6 \cdot 1 - 1)$, temos que $9 \mid 9$.
Passo Indutivo:
Suponha um arbitrário $k > 1 \in \mathbb{Z}$, tal que $9 \mid (4^k + 6k - 1)$. Ou seja, pela definição de divisibilidade:
(HI) $\exists w_1 \in \mathbb{Z}, (4^k + 6k - 1) = 9w_1$
- Portanto, *temos que provar que* $\exists w_2, 4^{k+1} + 6(k+1) - 1 = 9w_2$

$$\begin{aligned}4^{k+1} + 6(k+1) - 1 &= 4 \cdot 4^k + 6k + 6 - 1 \\ &= 3 \cdot 4^k + (4^k + 6k - 1) + 6, \text{ pois } 4 \cdot 4^k = 3 \cdot 4^k + 1 \cdot 4^k \\ &= (4^k + 6k - 1) + 3 \cdot 4^k + 6, \text{ ajustando os termos.} \\ &= 9w_1 + 3 \cdot 4^k + 6, \text{ pela HI.} \\ &= 9w_1 + 3(9w_1 - 6k + 1) + 6, \text{ pela HI, pois se segue de } 4^k = 9w_1 - 6k + 1. \\ &= 9w_1 + 27w_1 - 18k + 3 + 6 \\ &= 36w_1 - 18k + 9 \\ &= 9(4w_1 - 2k + 1) \\ &= 9w_2, \text{ onde } w_2 = 4w_1 - 2k + 1 \text{ e } w_2 \in \mathbb{Z}\end{aligned}$$

Pela definição de divisibilidade, temos que $9 \mid (4^{k+1} + 6 \cdot (k+1) - 1)$.
Portanto, é verdadeiro que $\forall n \in N,\ 9 \mid (4^n + 6n - 1)$.

2. Sabendo que o procedimento de criptografia RSA segue os seguintes passos:

Algorítmo para Geração de Chaves. A comunicação entre a Alice e o Beto é realizada da seguinte forma:
(1) Gere dois números primos aleatórios p e q (distintos)
(2) Calcule $n = p \cdot q$
(3) Calcule $\phi = (p-1) \cdot (q-1)$
(4) Escolha um número e, tal que $\text{mdc}(e, \phi) = 1$ e $1 < e < \phi$.
(5) Calcular o único número d (inverso de e módulo ϕ) $1 < d < \phi$, tal que $e \cdot d \equiv 1(\text{ mod } \phi)$.
(6) A chave privada é d e a chave pública é o par ordenado $< e, n >$.

Algorítmo para encriptar. Para encriptar uma mensagem m para Alice, Beto faz o seguinte:
(1) Obtem a chave pública (autêntica) de Alice (e, n)
(2) Representa a mensagem m como um inteiro em $\{0, 1, 2, ...n-1\}$.
(3) Calcula $c = m^e \text{ mod } n$
(4) Envia o texto encriptado c para Alice.

Algorítmo para desencriptar: Alice faz o seguinte com a mensagem de Beto:
Entrada: texto encriptado c, chave privada d
Saída: texto claro m Para recuperar o texto claro m a partir de c, Alice faz o seguinte:
(1) Utiliza a chave privada d para calcular o texto claro m:

$$m = c^d \text{ mod } n$$

Considere o sistema RSA com os seguintes parâmetros $p = 5, q = 23$ e $e = 27$.

(a) Determine as chaves **privada** e **pública** do usuário. **(_____/2,0 pts)**

Resposta: Chave pública: $(e, n) = (27, 115)$.
Chave privada: Calcular único inverso menor positivo de e módulo ϕ, tal que $e \cdot d \equiv 1(\text{ mod } \phi)$.

$$\begin{aligned}
27 &= 0 \cdot 88 + 27 \Longrightarrow 27 = 27 - 0 \cdot 88 \\
88 &= 3 \cdot 27 + 7 \Longrightarrow 7 = 88 - 3 \cdot 27 \\
27 &= 3 \cdot 7 + 6 \Longrightarrow 6 = 27 - 3 \cdot 7 \\
7 &= 1 \cdot 6 + 1 \Longrightarrow 1 = 7 - 1 \cdot 6 \\
6 &= 6 \cdot 1 + 0
\end{aligned}$$

Logo, $mdc(27, 88) = 1$.
Algorítmo para cálculo de MDC e constantes s e t do Teorema de Bézout:

a	b	b div a	b mod a	s'	t'	s=t'-s'(b div a)	t= s'
27	88	3	7	4	-1	-13	4
7	27	3	6	-1	1	4	-1
6	7	1	1	1	0	-1	1
1	6	6	0	0	1	1	0
0	1	-	-	-	-	0	1

Relação de Bézout: $mdc(27, 88) = 1 = (-13) \cdot 27 + 4 \cdot 88$. Dessa forma, o coeficiente s é -13.

Como a chave privada deve ser o único menor inverso positivo de e módulo ϕ) $1 < d < \phi$, tal que $27 \cdot d \equiv 1(\text{ mod } 88)$. Assim temos que calcular:

$$\begin{aligned}
-13 \text{ mod } 88 &= (-13) - \lfloor \tfrac{-13}{88} \rfloor \cdot 88 \\
&= (-13) - \lfloor (-0,14..) \rfloor \cdot 88 \\
&= (-13) - (-1) \cdot 88 \\
&= (-13) + 88 = 75.
\end{aligned}$$

$d = 75$.

(b) **Desencripte** o texto cifrado $c = 32$ para Alice. **(_____/3,0 pts)**

Nossa tarefa é desencriptar a cifra calculando com $d = 75, n = 115$ e $c = 32$:
$m = c^d \text{ mod } n$

Especificamente,

$32^{75} \text{ mod } 115$

Note que a base $32 = 2^5$. Assim, considerando que agora teremos o expoente $5 \cdot 75 = 375$. Aqui note que o módulo é co-primo com a base, $115 \perp 2$, assim usaremos o Teo. de Euler sabendo que

$$2^{\phi(115)} \equiv 1(\text{ mod } 115)$$

$$
\begin{aligned}
(2^5)^{75} \bmod 115 &= 2^{375} \bmod 115 \\
&= (2^{88})^4 \cdot 2^{23} \bmod 115, \text{ já que } 375 = 4 * 88 + 23 \\
&= 1^4 \cdot 2^{23} \bmod 115, \text{ dado que } 2^{\phi(115)} \equiv 1 \ (\bmod 115) \\
&= (2^1 \cdot 2^2 \cdot 2^4 \cdot 2^8 \cdot 2^8) \bmod 115, \text{ pois note que } 2^{23} = 2^1 \cdot 2^2 \cdot 2^4 \cdot 2^8 \cdot 2^8 \\
&= (2^1 \cdot 4 \cdot 16 \cdot 16^2 \cdot 16^2) \bmod 115 \\
&= (2^1 \cdot 4 \cdot 16 \cdot (256 \bmod 115) \cdot (256 \bmod 115)) \bmod 115 \\
&= (2^1 \cdot 64 \cdot 26 \cdot 26) \bmod 115 \\
&= (128 \cdot 26 \cdot 26) \bmod 115 \\
&= (13 \cdot 26 \cdot 26) \bmod 115 \\
&= (13 \cdot 101) \bmod 115 \\
&= 1313 \bmod 115 \\
&= 48
\end{aligned}
$$

3. Qual o menor valor positivo que satisfaz esta congruência linear? **(_____/1,0 pt)**

$$81x \equiv 12 \ (\text{mod } 264 \ )$$

Resposta: Note que 81, 12 e 264 são divisíveis por 3, e que $mdc(3, 264)$ é 3.

$$
\begin{aligned}
3 &= 0 \cdot 264 + 3 \\
264 &= 88 \cdot 3 + 0
\end{aligned}
$$

Portanto, convertemos nosso problema em:

$$27x \equiv 4 \ (\text{mod } 88 \ )$$

Pelo item (a) da questão anterior temos que o inverso positivo de 27 módulo 88 é 75. Portanto,

$$
\begin{aligned}
27x \cdot 75 &\equiv 4 \cdot 75 \ (\bmod 88 \ ) \\
x &\equiv 300 \ (\bmod 88 \ ), \text{ pois } 27 \cdot 75 \equiv 1 \ (\bmod 88 \ ) \\
x \bmod 88 &= 300 \bmod 88, \text{ pela definição de equivalência modular.} \\
x \bmod 88 &= 36
\end{aligned}
$$

4. Após muitos conflitos políticos no Brasil em 2019, os *illuminatis* decidem terceirizar uma intervenção militar e contratam um general chinês, que ficou encarregado de chefiar 500 soldados brasileiros antes de uma guerra civil, como para ele os ocidentais são todos muito parecidos, ele tinha uma certa dificuldade em contá-los. Seguindo uma intuição ancestral, após a guerra civil, o chinês alinhou os soldados em fileiras de 6 em 6 de forma que sobraram 3. Quando ele alinhou os soldados em fileiras de 7, também sobraram 3 soldados. Por fim, alinhou em fileiras de 11 e sobraram 5. Quantos soldados o general tinha no final? **(____/1 pt extra)**

Considerando,

$u = (u_1 \cdot M_1^{\varphi(m_1)} + u_2 \cdot M_2^{\varphi(m_2)} + ... + u_r \cdot M_r^{\varphi(m_r)}) \bmod m$

$m = 6 \cdot 7 \cdot 11 = 462$

$x \equiv 3 \ (\text{mod } 6 \ )$
$x \equiv 3 \ (\text{mod } 7 \ )$
$x \equiv 5 \ (\text{mod } 11 \ )$

$3 \cdot M_1 = 3 \cdot \left(\frac{m}{m_1}\right)^{\varphi(m_1)} = 3 \cdot \left(\frac{462}{6}\right)^{\varphi(6)} = 3 \cdot 77^2 \bmod 462 \ = 3 \cdot 5929 \bmod 462 \ = 231$

$3 \cdot M_2 = 3 \cdot \left(\frac{m}{m_2}\right)^{\varphi(m_2)} = 3 \cdot \left(\frac{462}{7}\right)^{\varphi(7)} = 3 \cdot 66^6 \bmod 462 \ = 3 \cdot (66^2)^3 = 3(4356)^3 \bmod 462 \ =$
$3 \cdot (198)^3 \bmod 462 \ =$
$3 \cdot 7762392 \bmod 462 \ = 3 \cdot 330 \bmod 462 \ = 66$

$5 \cdot M_3 = 5 \cdot \left(\frac{m}{m_3}\right)^{\varphi(m_3)} = 5 \cdot \left(\frac{462}{11}\right)^{\varphi(11)} \bmod 462 \ = 5 \cdot 42^{10} \bmod 462 \ = 5 \cdot (42^2)^5 \bmod 462 \ =$
$5 \cdot 1764^5 \bmod 462 \ = (5 \cdot 378^2 \cdot 378^3) \bmod 462 \ = (5 \cdot 126 \cdot 42) \bmod 462 \ = (168 \cdot 42) \bmod 462 \ =$
$7056 \bmod 462 \ = 126$

$x = (231 + 66 + 126) \bmod 462 \ = 423$

Verificando temos que
$423 \bmod 6 = 3$
$423 \bmod 7 = 3$
$423 \bmod 11 = 5$

Portanto, ficaram 423 soldados.

— Propriedades e Teoremas —

- **Soma modular.** Sejam a, b e n inteiros e $n > 1$, então

$$a + b \equiv ((a \textbf{ mod } n) + (b \textbf{ mod } n)) \textbf{ mod } n$$

- **Multiplicação modular.** Sejam a, b e n inteiros e $n > 1$, então

$$a \cdot b \equiv ((a \textbf{ mod } n) \cdot (b \textbf{ mod } n)) \textbf{ mod } n$$

- **Exponenciação modular.** Sejam a, b e n inteiros e $n > 1$, então

$$a^m \equiv ((a \textbf{ mod } n)^m) \textbf{ mod } n$$

- **Regra do cancelamento I.** Sejam $a, b, c, n \in Z$, com $n > 0$. Se $c \perp n$, então

$$ac \equiv bc \pmod{n} \text{ se, e somente se, } a \equiv b \pmod{n}$$

- **Regra do cancelamento II.** Sejam a, b, c, n inteiros, com $n > 0$, então

$$ac \equiv bc \pmod{n} \text{ se, e somente se, } a \equiv b \pmod{\frac{n}{\text{mdc}(c,\ n)}}$$

- **Resolvendo Congruências Lineares.** Sejam a, b, n inteiros, com $n > 0$, e seja $d := \text{mdc}(a, n)$. Se $d \mid b$, então a congruência $ax \equiv b \pmod{n}$ possui uma solução x, e qualquer inteiro x' é também solução se e somente se $x \equiv x' \pmod{\frac{n}{d}}$.
- **Inverso Modular.** Dizemos que, para um inteiro positivo n e um inteiro a, temos que a_n^{-1} é o **inverso de a módulo n** se este é o menor inteiro positivo que satisfaz

$$a \cdot a_n^{-1} \equiv 1 \pmod{n}$$

- **Pequeno Teorema de Fermat.** Para qualquer número primo p e $a \in Z$, sendo $p \nmid a$, então

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

- **Método de computar a Totiente**. Se $n = p_i^{e_1} ... \ p_r^{e_r}$ é a fatoração de n em primos, então

$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) = n \prod_{i=1}^{r}(1 - \frac{1}{p_i})$$

- **Teorema de Euler.** Para quaisquer $a, n \in Z$, sendo $n > 0$ e $a \perp n$, então

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

- **Teorema Chinês dos Restos.** Sejam $m_1, m_2, ..., m_r$ inteiros positivos tal que

$$m_j \perp m_k, \text{ quando } j \neq k$$

  Sejam $u_1, u_2, ..., u_r$ inteiros, então há um único inteiro u que satisfaça as condições

$$0 \leq u < m \quad \text{e} \quad u \equiv u_j \pmod{m_j}, \text{ para } 1 \leq j \leq r$$

  Assim, o número que satisfaz tais condições é

$$u = (u_1 \cdot M_1^{\varphi(m_1)} + u_2 \cdot M_2^{\varphi(m_2)} + ... + u_r \cdot M_r^{\varphi(m_r)}) \bmod m$$

  em que $m = \prod_{i=1}^{r} m_i$, $M_i = \frac{m}{m_i}$
  Alternativamente, o número pode ser determinado como

$$u = u_1 \cdot M_1 \cdot y_1 + u_2 \cdot M_2 \cdot y_2 + ... + u_r \cdot M_r \cdot y_r \bmod m$$

  em que $m = \prod_{i=1}^{r} m_i$, $M_i = \frac{m}{m_i}$ e y_i é o inverso de $M_i \bmod m$