



Universidade de Brasília
Faculdade do Gama

Matemática Discreta 2

Prof. Dr. Glauco Vitor Pedrosa



Exercício

Verifique se:

a) $3 \mid 5^{2011} + 2 \cdot 11^{2011}$

b) $2 \mid 3^n + 1$

c) $3 \mid 2^{2n} - 1$

d) $8 \mid 9^n - 8n - 1$

e) $64 \mid 3^{2n+2} - 8n - 9$

Exercício

Achar o resto da divisão de:

a) 2^{257} por 7

b) 3^{23456} por 13

c) $15!$ por 17

Inverso modular

- Seja \underline{a} um inteiro. Chama-se **inverso multiplicativo** de \underline{a} *módulo* \underline{m} um inteiro \underline{a}^* tal que:

$$\underline{a} \cdot \underline{a}^* \equiv 1 \pmod{m}$$

ATENÇÃO: Só existe inverso modular se $\text{mdc}(a,m) = 1$

Exemplo: encontre o inverso modular das seguintes congruências:

a) $3 \pmod{7}$ **Resposta: 5, pois $3 \cdot 5 \equiv 1 \pmod{7}$**

b) $6 \pmod{17}$ **Resposta: 3, pois $6 \cdot 3 \equiv 1 \pmod{17}$**

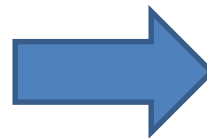
c) $5 \pmod{8}$ **Resposta: 5, pois $5 \cdot 5 \equiv 1 \pmod{8}$**

Inverso modular

- Como encontrar o inverso modular?

Exemplo: **32 (mod 51)**

	q	1	1	1	2	6
	51	32	19	13	6	1
r	19	13	6	1	0	



q	mn
-	1
2	2
1	3
1	5
1	8

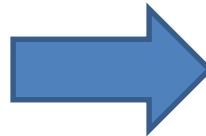
De fato: $32 \cdot 8 \equiv 1 \pmod{51}$
 $256 \equiv 1 \pmod{51}$

Inverso modular

- Como encontrar o inverso modular?

Exemplo: **3 (mod 10)**

	q	3	3
	10	3	1
r	1	0	



q	mn
-	1
3	3



Quando a quantidade de quocientes nesta
coluna for ímpar, então devemos fazer:



$$10 - 3 = \boxed{7}$$

De fato: $7 \cdot 3 \equiv 1 \pmod{10}$

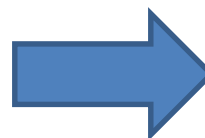
$$21 \equiv 1 \pmod{10}$$

Inverso modular

- Como encontrar o inverso modular?

Exemplo: **17 (mod 27)**

	q	1	1	1	2	3
	27	17	10	7	3	1
r	10	7	3	1	0	



q	mn
-	1
2	2
1	3
1	5
1	8

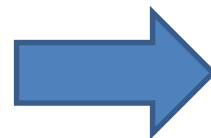
De fato: $8 \cdot 17 \equiv 1 \pmod{27}$
 $136 \equiv 1 \pmod{27}$

Inverso modular

- Como encontrar o inverso modular?

Exemplo: **5 (mod 39)**

	q	7	1	4
	39	5	4	1
r	4	1	0	



q	mn
-	1
1	1
7	8

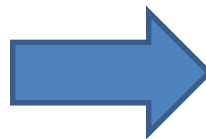
De fato: $5 \cdot 8 \equiv 1 \pmod{39}$
 $40 \equiv 1 \pmod{39}$

Inverso modular

- Como encontrar o inverso modular?

Exemplo: **37 (mod 41)**

	q	1	9	4
	41	37	4	1
r	4	1	0	



q	mn
-	1
1	1
9	10

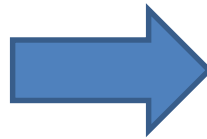
De fato: $37 \cdot 10 \equiv 1 \pmod{41}$
 $370 \equiv 1 \pmod{41}$

Inverso modular

- Como encontrar o inverso modular?

Exemplo: **35 (mod 51)**

	q	1	2	5	3
	51	35	16	3	1
r	16	3	1	0	



q	mn
-	1
5	5
2	11
1	16



Quando a quantidade de quocientes nesta coluna for ímpar, então devemos fazer:



$$51 - 16 = \boxed{35}$$

$$\text{De fato: } 35 * 35 \equiv 1 \pmod{51}$$

$$1225 \equiv 1 \pmod{51}$$

Congruências Lineares

- Chama-se **congruência linear** toda equação da forma:

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

onde a e b são dois inteiros quaisquer e m um inteiro positivo

Todo inteiro x_0 tal que

$$ax_0 \equiv b \pmod{m}$$

diz-se uma *solução* da congruência linear

Congruências Lineares

- **Exemplo**

Dada a seguinte congruência linear

$$3x \equiv 2 \pmod{4}$$

Qual seria um valor de x que satisfaz a congruência linear acima?

Congruências Lineares

- Se $ax \equiv b \pmod{m}$, então $m \mid (ax-b)$, ou seja:
$$ax - b = m.y$$
$$ax - my = b \Rightarrow \text{equação diofantina}$$

Exemplo:

Para resolver a seguinte congruência linear:

$$11x \equiv 2 \pmod{317}$$

Basta resolver a seguinte equação diofantina:

$$11x - 317y = 2$$

A solução geral para a equação diofantina acima é:

$$x = -288 - 317t$$

Para $x > 0$, temos que $t < -0,90$, ou seja $t = -1$

De fato, para $t = -1$, temos que $x = 29$, que é uma solução da congruência

Congruências Lineares

Outro exemplo:

Para resolver a seguinte congruência linear:

$$3x \equiv 1 \pmod{5}$$

Basta resolver a seguinte equação diofantina:

$$3x - 5y = 1$$

A equação diofantina acima tem a seguinte solução geral:

$$x = 2 - 5t$$

Para $x > 0$, temos que $t < 0,4$.

De fato, para $t = 0$, temos **$x = 2$** que é uma solução da congruência linear.

Congruências Lineares

Outro exemplo:

Para resolver a seguinte congruência linear:

$$18x \equiv 30 \pmod{42}$$

Basta resolver a seguinte equação diofantina:

$$18x - 42y = 30$$

A equação diofantina acima tem a seguinte solução geral:

$$x = -10 - 7t$$

Para $x > 0$, temos que $t < -1,428\dots$

De fato, para $t = -2$, temos **$x = 4$** que é uma solução da congruência linear.

Congruências Lineares

Outro exemplo:

Para resolver a seguinte congruência linear:

$$21x \equiv 15 \pmod{39}$$

Basta resolver a seguinte equação diofantina:

$$21x - 39y = 15$$

A equação diofantina acima tem a seguinte solução geral:

$$x = 10 - 13t$$

Para $x > 0$, temos que $t < 0,769...$

De fato, para $t = 0$, temos **$x = 10$** que é uma solução da congruência linear.

Congruências Lineares

Outro exemplo:

Para resolver a seguinte congruência linear:

$$35x \equiv 5 \pmod{14}$$

Basta resolver a seguinte equação diofantina:

$$35x - 14y = 5$$

A equação diofantina acima não tem solução, pois $\text{mdc}(35, 14) = 7$ e $7 \nmid 5$, logo a **congruência não tem solução!**

Exercício

- Achar todos os inteiros x tal que:
 $0 < x < 15$ e $3x \equiv 6 \pmod{15}$

Resposta: 2, 7 e 12.