/ /

UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 16 de Março de 2017

- MAIS UM EXEMPLO DO EUCLIDIANO ESTENDIDO

MDC (7648, 122) = ?

RESTO	QUOCIENTE	x ou α	y ou β
7648	—	1	0
122	—	0	1
84	62	1-62·0 = 1	0-62·1 = -62
38	1	0-1·1 = -1	1-1·(-62) = 63
8	2	1-2·(-1) = 3	-62-2·63 = -188
6	4	-1-4·3 = -13	63-4·(-188) = 815
2	1	3-1·(-13) = 16	-188-1·815 = -1003
0	3	—	—

$\alpha \cdot a + \beta \cdot b = d = MDC(a,b) \rightarrow 16 \cdot 7648 - 1003 \cdot 122 = 2$

O Algoritmo Euclidiano Estendido nos oferece um método para obter um valor de α e um valor de β que satisfazem a equação:

$$\alpha \cdot a + \beta \cdot b = d = MDC(a,b)$$

Entretanto, estes valores de α e β não são únicos. Existem, literalmente, infinitos valores para α e β que satisfazem esta equação. Sejam α_0 e β_0 os valores calculados pelo A.E.E (Algoritmo Euclidiano Estendido).

Vamos definir

$$\begin{cases} \alpha_k = \alpha_0 - k \cdot b \ (k \in \mathbb{Z}) \\ \beta_k = \beta_0 + k \cdot a \end{cases}$$

Cada par α_k e β_k satisfaz a equação.

$$\alpha_k \cdot a + \beta_k \cdot b =$$
$$= (\alpha_0 - kb)a + (\beta_0 + ka)b =$$
$$= \alpha_0 a - kba + \beta_0 b + kab =$$
$$= \alpha_0 a + \beta_0 b = d = MDC(a,b)$$

- O A.E.E SEMPRE TERMINA?

A condição de parada do A.E.E é a mesma do Algoritmo Euclidiano Comum (para quando encontra um resto zero). Como já vimos que o Algoritmo Euclidiano sempre termina, o mesmo vale para o A.E.E

- O A.E.E PRODUZ O RESULTADO CORRETO?

1) O cálculo do MDC no A.E.E é idêntico ao do Algoritmo Euclidiano Comum, que já vimos ser correto.

2) O cálculo de α e β também é correto, pois a corretude é verificada a cada passo pelo uso das equações calculadas algébricamente.

- EQUAÇÕES DIOFANTINAS

↳ São equações em que todos os coeficientes são inteiros e todas as variáveis também precisam sempre assumir valores inteiros.

- EXEMPLO: $2x = 3$ não tem solução quando pensada como equação diofantina.

↳ Podemos utilizar o A.E.E para resolver equações diofantinas lineares com 2 variáveis:

$$\begin{cases} ax+by=c \\ a,b,c \in \mathbb{Z} \\ x \text{ e } y \text{ só podem assumir valores inteiros} \end{cases}$$

Suponha que x_0 e y_0 formam uma solução para a equação

$$ax+by=c$$

Isto é,

$$ax_0+by_0=c$$

Seja $d = MDC(a,b)$ → $a = d \cdot a'$ e → $b = d \cdot b'$

$$da' \cdot x_0 + db' y_0 = c$$

$$d(a' x_0 + b' \cdot y_0) = c$$

d DIVIDE c

Conclusão: Se a equação $ax+by=c$ possui solução inteira, então o MDC dos coeficientes a e b divide também o coeficiente c.

Suponha agora que $d = MDC(a,b)$ divide o coeficiente c.

$$c = d \cdot c'$$

Vamos aplicar o A.E.E a a e b. Obtemos então dois inteiros α e β tais que

$$\alpha \cdot a + \beta b = d$$

↓ MULTIPLICO ESSA EQUAÇÃO POR c'

$$\alpha \cdot a \cdot c' + \beta \cdot b \cdot c' = dc' = c$$

$$a \cdot (\alpha c') + b(\beta \cdot c') = c$$

Logo,

$$\begin{cases} x = \alpha \cdot c' \\ y = \beta \cdot c' \end{cases}$$

é uma solução para a equação $ax + by = c$.

Conclusão 2: Se o MDC(a,b) divide o coeficiente c, então a equação $ax + by = c$ possui solução inteira.

Conclusão 1 + Conclusão 2 $\Rightarrow$ A equação $ax + by = c$ possui solução inteira se e somente se $d = MDC(a,b)$ também divide o coeficiente c.

- Receita para usar o A.E.E para resolver estas equações diofantinas:

1) São dados os coeficientes a, b e c da equação.

2) Aplico o A.E.E a a e b. Obtenho:
   - $d = MDC(a,b)$
   - α
   - β

3) Testo se d divide c.
   - Na prática, calculo o quociente c' e o resto r da divisão de c por d.

4) Se d não divide c (se $r \neq 0$) então a equação não tem solução inteira.

5) Se d divide c (se $r = 0$), então:
$x = \alpha \cdot c'$ e $y = \beta \cdot c'$
é uma solução inteira para equação

/ /

Exemplo 1. $762x + 18y = 6$

- A.E.E

R	Q	α	β
762	-	1	0
18	-	0	1
6	42	1	-42
0	3	-	-

$d = 6$

$\alpha = 1$

$\beta = -42$

- Divido c por d

- Quociente $c' = 1$

- Resto $r = 0$

$x = \alpha \cdot c' = 1$

$y = \beta \cdot c' = -42$

Exemplo 2: $762x + 18y = 30$

- Divido c por d

- Quociente $c' = 5$

- Resto $r = 0$

$x = \alpha \cdot c' = 1 \cdot 5 = 5$

$y = \beta \cdot c' = -42 \cdot 5 = -210$

Exemplo 3: $1361x + 900y = 1$

R	Q	α	β
1361	-	1	0
900	-	0	1
461	1	1	-1
158	2	-2	3
85	2	5	-7
73	1	-7	10
12	1	12	-17
1	6	-79	112
0	12	-	-

$d = 1$

$\alpha = -79$

$\beta = 112$

- Divido c por d:
  - Quociente $c' = 4$
  - Resto $r = 0$

$x = \alpha \cdot c' = -79 \cdot 4 = -316$

$y = \beta \cdot c' = 112 \cdot 4 = 448$

Exemplo 4: $76x + 980y = 7$

R	Q	α	β
76	-	1	0
980	-	0	1
76	0	1	0
68	12	-12	1
8	1	13	-1
4	8	-116	9
0	2	-	-

$d = 4$

$\alpha = -116$

$\beta = 9$

- Dividindo c por d:

↳ Quociente $c' = 1$

↳ Resto $r = 3$

↓

A equação não tem solução inteira.

- Numero primo: um número primo é um número inteiro positivo, maior ou igual a 2 que possui como divisores apenas 1 e ele mesmo

- OBS 1: Um número inteiro positivo maior ou igual a 2 que não é primo é um número composto.

- OBS 2: 1 não é primo nem é composto.

- Teorema fundamental da aritmética (Teorema da fatoração única):

Seja $n \geq 2$ um número inteiro. Então, existe uma fatoração

$$n = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k},$$

onde $p_1 < p_2 < \dots < p_k$ são primos e $l_i \geq 1$, para todo $1 \leq i \leq k$. Além disso, essa fatoração é única.

Os números $p_1, p_2, \dots, p_k$ são os fatores primos de n.

Os números $l_1, l_2, \dots, l_k$ são as multiplicidades dos fatores primos

Exemplos: $n = 18$ | $n = 64$ | $n = 24$

$n = 2 \cdot 3^2$ | $n = 2^6$ | $n = 2^3 \cdot 3$

/ /

- DUAS PARTES NO TEOREMA:

1) EXISTÊNCIA

↳ ALGORITMOS DE FATORAÇÃO:

↳ ALGORITMO "INGÊNUO"

↳ ALGORITMO DE FERMAT

2) UNICIDADE

↳ FAREMOS UMA PROVA POR CONTRADIÇÃO.