NÚMEROS INTEIROS E CRIPTOGRAFIA – UFRJ

GABARITO LISTA 1: ALGORITMOS BÁSICOS - 2016.1

Gabarito preparado por Rennan Gaio (monitor 2015-1 e 2016-1)

1. gabarito no livro
2. Ache *infinitas* soluções inteiras da equação $23303x + 2359y = 21$.

   Aplicando o algoritmo euclidiano estendido, temos

Restos	Quocientes	x
23303	*	1
2359	*	0
2072	9	1
287	1	-1
63	7	8
35	4	-33
28	1	41
7	1	-74
0	*	*

   Como $23303x + 2359y = 7$ e $x = -74$, então

$$y = \frac{7 - 23303 \cdot -74}{2359} = 731.$$

   Logo

$$23303 \cdot -74 + 2359 \cdot 731 = 7,$$

   e multiplicando tudo por 3 obtemos

$$23303 \cdot -74 \cdot 3 + 2359 \cdot 731 \cdot 3 = 21.$$

   Portanto, as soluções inteiras são

$$23303 \cdot (-74 \cdot 3 - 2359k) + 2359 \cdot (731 \cdot 3 + 23303k) = 21.$$

3. Determine múltiplos de 330 e de 240 cuja soma seja 210.

   Solução semelhante ao segundo exercício: $21 \cdot 330$ e $28 \cdot 240$

4. Determine o máximo divisor comum entre $p^2 - p + 1$ e $(p^2)! + 1$, sabendo-se que p é um primo positivo. De que modo a resposta depende de p?

   Como $p^2! + 1 > p^2 - p + 1$, vamos dividir o primeiro pelo segundo, como no algoritmo euclidiano estendido. Obtemos

   $$p^2! + 1 = (p^2 - p + 1)(p^2 + 1)! + p(p^2 - 1)! - (p^2 - 1)! + 1)$$

   Portanto, pelo resultado auxiliar usado na demonstração do algoritmo euclidiano:

   $$\text{mdc}(p^2! + 1, p^2 - p + 1) = \text{mdc}(p^2 - p + 1, (p^2 - 1)!(p - 1) + 1).$$

   Como p é um primo positivo, ele eḿaior que 1. Logo $p^2 - p + 1$ é um fator de $(p^2 - 1)!$. Logo o mdc entre eles é igual a 1.

5. Determine números inteiros x e y que sejam soluções da equação $7001x + 503y = 2$ e prove que esta equação tem infinitas soluções inteiras.

   Semelhante ao segundo exercício; a solução geral é dada por

   $$x = 368 \cdot 7001 + 503 \cdot k \quad \text{e} \quad y = -5122 \cdot 503 - 7001 \cdot k.$$

6. Seja $n > 2^{100!}$ um número inteiro. Determine $\text{mdc}(6n+1, 6n!+(n-1)!+6n-3)$.

   Como $6n!+(n-1)!+6n-3 > 6n+1$, vamos dividir o primeiro pelo segundo, como no algoritmo euclidiano estendido. Obtemos $6n! + (n-1)! + 6n - 3 = (6n + 1)(n - 1)! + 6n - 3$. Portanto, pelo resultado auxiliar,

   $$\text{mdc}(6n + 1, 6n! + (n - 1)! + 6n - 3) = \text{mdc}(6n + 1, 6n - 3).$$

   Como $6n + 1 = 6n - 3 + 4$, segue pelo resultado auxiliar mais uma vez que $\text{mdc}(6n + 1, 6n - 3) = \text{mdc}(6n - 3, 4)$. Mas $6n - 3 = 3(2n - 1)$, que é um número ímpar. Como 4 é uma potência de 2, não pode haver nenhum fator maior que 1 comum a $6n - 3$ e 4. Logo $\text{mdc}(6n + 1, 6n - 3) = 1$.

   Outra maneira de calcular $\text{mdc}(6n - 3, 4)$ (baseada na solução de Moyses Afonso Assad Cohen). Podemos considerar dois casos. No primeiro caso n é par e podemos escrevê-lo na forma $n = 2k$. Neste caso, precisamos calcular $\text{mdc}(12k - 3, 4)$. Mas, dividindo $12k - 3$ por 4, obtemos

   $$12k - 3 = 4 \cdot 4k - 3$$

de modo que, pelo resultado auxiliar visto em aula,

$$\text{mdc}(12k-3,4) = \text{mdc}(-3,4) = \text{mdc}(3,4) = 1.$$

No segundo caso n é ímpar, de modo que $n = 2k+1$. Então, precisamos calcular $\text{mdc}(12k+3,4)$. Mas repetindo um argumento semelhante ao anterior, verificamos que

$$\text{mdc}(12k+3,4) = \text{mdc}(3,4),$$

de modo que $\text{mdc}(12k+3,4) = 1$. Portanto, independente de n ser par ou ímpar, temos que

$$\text{mdc}(6n-3,4) = 1.$$

7. Seja $n > 2^{100!}$ um número inteiro. Use o algoritmo euclidiano estendido para calcular $d = \text{mdc}(5n+3, 3n+2)$ e dois inteiros α e β tais que $d = (5n+3)\alpha + (3n+2)\beta$.

Aplicando o algoritmo euclidiano estendido, temos

Restos	Quocientes	x
$5n+3$	*	1
$3n+2$	*	0
$2n+1$	1	1
$n+1$	1	-1
n	1	2
1	1	-3
0	*	*

Logo, temos $d = 1$ e α = -3. Para descobrirmos a valor de β basta fazermos:

$$\beta = \frac{1-(5n+2)\cdot\alpha}{3n+2} = 5.$$

8. Determine $\text{mdc}(a,c)$ sabendo-se que a, b e c são inteiros maiores que $2^{200!}$ e que c divide $a+b$ e $\text{mdc}(a,b) = 1$.

Seja $d = \text{mdc}(a,c)$. Então,

$$a = da' \quad \text{e} \quad c = dc'$$

em que $a', c' \in \mathbb{Z}$. Substituindo em $a+b = ck$, obtemos $da' + b = (dc')k$, donde $b = d(c'k - a')$. Mas isto significa que d divide b. Como d também divide a, concluímos que d é divisor comum de a e b. Contudo, o máximo

divisor comum de a e b é 1. Assim, $0 < d \leq 1$, de modo que $d = 1$ é o mdc desejado.

9. Use o algoritmo euclidiano estendido para determinar um inteiro a de modo que $6765 \cdot a - 1$ seja divísivel por 10946.

   Queremos que:
   $$6765 \cdot a - 1 = 10946 \cdot k;$$
   que equivale a
   $$6765 \cdot a - k \cdot 10946 = 1.$$
   Fazendo $k = -j$, obtemos
   $$6765 \cdot a + j \cdot 10946 = 1.$$
   Agora só precisamos aplicar o algoritmo euclidiano estendido. Usando a como x e o j como y, temos:

Restos	Quocientes	x
6765	*	1
10946	*	0
6765	0	1
4185	1	-1
2580	1	2
1605	1	-3
975	1	5
630	1	-8
345	1	13
285	1	-21
60	1	34
45	4	-157
15	1	191

   Logo 191 é um valor que a pode assumir.

10. Qual o valor do d correspondente à chave de RSA que tem n igual ao produto dos primos $p = 4327$ e $q = 8329$ e para a qual $e = 6752489$?

    Sabendo que $(p-1) \cdot (q-1) \cdot g + e \cdot d = 1$, temos que:
    $$36026928 \cdot k + 6752489 \cdot d = 1.$$

Aplicando agora o algorítimo euclidiano estendido:

Restos	Quocientes	x
36026928	**	1
6752489	**	0
2264483	5	1
2223523	2	- 2
40960	1	3
11683	54	- 164
5911	3	495
5772	1	- 659
139	1	1154
73	41	- 47973
66	1	49127
7	1	- 97100
3	9	923027
1	2	- 1943154

Como

$$y = \frac{1 - 36026928 \cdot (-1943154)}{6752489} = 10367417$$

é positivo, temos que

$$d = 10367417.$$

Se você encontrar algum erro no gabarito, por favor comunique ao professor através do endereço `collier@dcc.ufrj.br`. Qualquer dúvida entre em contato com os monitores via FaceBook. As aulas de monitoria serão nas segundas-feiras 13h-15h