Números Inteiros e Criptografia, PLE 2020 - Lista de Exercícios 4
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049873

Questão 1.

a. Ache um múltiplo de 330 e um múltiplo de 240 cuja soma seja 210.
Para um múltiplo de 330 temos: a = 330q
E para um múltiplo de 240 temos: b = 240q’

Logo procuramos números que satisfaçam a+b=210

Substituindo, temos: 330q + 240q’ = 210, que simplificado vira
11q + 8q’ = 7

Achamos que um dos valores de q e q’ seria -3 e 5
11(-3) + 8(5) =
-33 + 40 = 7

Substituindo nos múltiplos:
a = 330(-3) = -990
b= 240(5) = 1200

Logo, temos que o múltiplo de 330 e o múltiplo de 240 cuja soma seja 210 é, respectivamente, -990 e 1200.

b. Mostre que existem infinitas soluções para o item anterior.
Do exercício anterior temos que 330q+240q’ = 210, que podemos ler como $\alpha(a) + \beta(b) = d$, sendo ‘a’ e ‘b’ inteiros positivos e ‘d’ seu mdc, como não há limitações para os valores de $\alpha$ e $\beta$, temos que o resultado ‘d’ pode ser obtido de infinitas maneiras.

Questão 2.
Em Brasilândia, o jogo de basquete é jogado com regras diferentes. Existem apenas dois tipos de pontuações para as cestas: 5 e 11 pontos. É possível uma pontuação entre dois times de 86 × 39?

Do enunciado podemos tirar:
5x + 11y = 86
5x+ 11y = 39
Sendo x e y o número de cestas das respectivas pontuações.

5x + 11y = 86 é possível visto que se forem marcadas 4 cestas de 5 pontos e 6 cestas de 11 pontos nós teremos:
5(4) + 11(6) =
20 + 66 = 86

Entretanto, para 5x+ 11y = 39 teríamos que ter y=9 ou y=4(dependendo do x) para chegarmos a 9 pontos na casa das unidades, mas isso nos daria 90 pontos ou 40 pontos, o que é maior que 39, e como não há como fazer “cestas negativas” para diminuir esse número, torna-se impossível fazer 39 pontos com as cestas valento esse pontos.

Questão 3.
Sejam a natural e p primo. Fazendo uma análise (completa) de casos, determine todos os possíveis valores de mdc(a, p^2 ) (em função de a e/ou de p).

Para achar os valores de mdc(a, p^2), nós utilizamos o final do algoritmo de euclides, com resto zero;

a = p^2(q) + 0

Assim os valores possíveis para o mdc são aqueles que são iguais a ‘a’ quando este for múltiplo de p^2.

Questão 5.
Seja n > 0 um número inteiro positivo composto e p seu menor fator primo. Sabe-se que p ≥ √ n e que p − 4 divide mdc(6n + 7, 3n + 2). Determine todos os possíveis valores de n.

p ≥ √ n é igual a p^2 ≥ n

Assumindo que p^2 é o menor fator de n temos que n = (p^2)q e isso só será possível caso q = 1, tornando p^2 = n

p-4 | mdc(6n + 7, 3n + 2)

Achando o mdc pelo algoritmo de Euclides:
6n+7 = 3n+2(Qo) + Ro
6n+7 = 3n+2(2) + 3
3n+2 = 3(n) + 2
2 = 2(1) + 1
2 = 1(2) + 0

mdc(6n + 7, 3n + 2) = 1

temos então que p - 4 divide 1:

p-4 | 1

1 = (p-4)q

Para que isso seja possível, q=1 ou q= -1

Caso q=1:
1=p-4

$p = 5$

Caso $q = -1$:

$1 = -p+4$

$p = 3$

Como $p^2 = n$, encontramos que os valores de n são 25 e 9

Questão 6.
Mostre que existe um inteiro múltiplo de $241^2$ que termina em 241 (Dica: Observe que um número termina em 241 se ele é da forma $1000n + 241$, com n natural).

Temos pelo enunciado que:
$1000n + 241$ é um número que termina em 241 e precisamos mostrar que ele é múltiplo de $241^2$.

Logo
$241^2 \mid 1000n + 241$

$1000n + 241 = (241^2)q$

$1000n = (241^2)q - 241$

Colocando 241 em evidência:

$1000n = 241(241q - 1)$

Temos agora que

$1000n/241 = 241q - 1$

Chamando $n/241$ de d, chegamos em

$1000d = 241q - 1$

$241q = 1000d + 1$

Assim temos que $1000d + 1$ é um número terminado em 001

Logo, temos que achar um número que multiplicado por 241 dê um número terminado em 001:

Fazendo $q = xy1$, chegamos em $241 * aq1$ e resolvendo essa multiplicação:

```
          2   4   1
          x   y   1
     --------------------- x
          2   4   1
     2y  4y   y   0
2x   4x   x   0   0   +
---------------------------
  ……… 0   0   1
```

Para que nessa soma cheguemos em 001, no final y deve ser igual a 6 e consequentemente x deve ser igual 3. Dessa forma achamos que q=361, onde (241^2)*361 = 20967241, sendo este um múltiplo de 241^2 terminado em 241.

Questão 7.
O Algoritmo Euclidiano funciona tão bem que é difícil encontrar pares de números que o fazem demorar muito.
a. Encontre dois números cujo mdc é 1, para os quais o Algoritmo Euclidiano demora 5 passos (vamos contar cada divisão efetuada como sendo 1 passo).

Podemos chegar nos dois números fazendo o Algoritmo Euclidiano ao contrário. No final do algoritmo encontramos o mdc dos números iniciais igual a 1 e o resto igual a zero.

a = b * (q) + r, onde b = 1 e q = 0
a = 1 * (q) + 0

Chutando um valor para começar, nesse caso o 7:

7 = 1 * (7) + 0

Com isso podemos voltar o 7 como divisor e o 1 como resto.

a = 7 * (q) + 1

escolhemos um q e encontramos a. Para q=7 teremos:

50 = 7*(7) + 1

e assim seguimos o algoritmo inverso que ficará assim:

7 = 1 * (7) + 0
50 = 7*(7) + 1
207 = 50 * (4) + 7
671 = 207 * (3) + 50
1549 = 671 * (2) + 207
8416 = 1549 * (5) + 671

Encontramos assim que os dois números em que o algoritmo euclidiano demora 5 passos para achar o mdc igual a 1 são 8416 e 1549.

b. Encontre dois números cujo mdc é 1, para os quais o Algoritmo Euclidiano demora 6 passos (dica: estenda a ideia que você usou na letra a).

Continuando o algoritmo inverso:

7 = 1 * (7) + 0
50 = 7*(7) + 1
207 = 50 * (4) + 7
671 = 207 * (3) + 50
1549 = 671 * (2) + 207
8416 = 1549 * (5) + 671
26749 = 8416 * (3) + 1549

Sendo assim, 26749 e 8416 os números em que o algoritmo euclidiano demora 6 passos para encontrar o mdc igual a 1.

c. Descreva um método para resolver o seguinte problema: dado um natural k, encontrar dois números cujo mdc é 1, para os quais o Algoritmo Euclidiano demora k passos

O processo já foi descrito na letra a) deste exercício.
Começamos com o final do algoritmo euclidiano, com resto 0 e mdc igual a 1.
Depois escolhemos o dividendo e o quociente iguais para que a igualdade seja verdadeira.
O próximo passo é usar o antigo divisor como o nosso novo resto e nosso antigo dividendo como nosso novo divisor.
Assim fazemos k passos pedidos, depois de k passos nossos números cujo mdc é igual a 1 serão nossos dividendo e divisor daquele último passo.

Questão 9.
Sejam a, b, c e d números naturais. Prove ou refute com um contraexemplo.
a. Se c = mdc(a, b) e x = ab, então c^2 | x.

c = mdc(a, b) ^ x = ab → c^2 | x

Dessa forma temos que:
c ^ 2 | ab

ab = c^2(q), fazendo ab=c(cq) → ab =c(q’)

pela contrapositiva:

¬ (c^2 | x) → ¬ ( c = mdc(a, b) ^ x = ab)

$\neg (x = c^2(q)) \rightarrow \neg c = mdc(a,b) \wedge \neg x=ab$

O que é verdade, visto que x não seria mais um múltiplo de c^2, que por sua vez também não é múltiplo de c.

b. (a | b ou a | c) sse a | bc

$a|b \vee a|c \leftarrow\rightarrow a|bc$

$(\rightarrow)$
a|b : b = aq

a|c : c = aq'

a| bc : bc = aq''

Substituindo:
(aq)(aq') = aq''
qq' = q''

Sendo assim só mais um número multiplicando 'a', provando que se 'a' divide b ou 'a' divide 'c', então 'a' divide a sua multiplicação.

$(\leftarrow)$

$a|bc \rightarrow a|b \vee a|c$

$bc = aq'' \rightarrow b = aq \vee c = aq'$

temos que b = aq''/c e c = aq''/b

Substituindo

aq''/c = aq
q'' = qc, sendo c um natural

aq''/b = aq'
q'' =q'b, sendo b um natural

Sendo assim q'' apenas um múltiplo dos outros q e q'

se 'a' divide bc, então ele divide b ou de c.

Questão 10.
O mínimo múltiplo comum de a e b é o menor inteiro positivo que é múltiplo de a e que é múltiplo de b. Vamos denotar esse número por mmc(a, b). Prove as seguintes afirmações.

a. mmc(a, b) · mdc(a, b) = ab.

Dica: mostre separadamente que mmc(a, b) · mdc(a, b) ≥ a · b e mmc(a, b) · mdc(a, b) ≤ a · b. Lembre-se: mdc(a, b) é definido como o máximo . . ., o que nos dá uma estratégia para concluirmos que mdc(a, b) é maior ou igual a um dado inteiro; analogamente, mmc(a, b) é definido como o mínimo . . ., o que nos dá uma estratégia para concluirmos que mmc(a, b) é menor ou igual a um dado inteiro. Em uma dessas provas, utilize o item c abaixo (você pode usá-lo mesmo se não conseguir prová-lo).

b. mmc(a, b) = ab sse mdc(a, b) = 1.

mmc(a, b) = ab ← → mdc(a, b) = 1

( → )

temos pelo algoritmo euclidiano com resto igual a 0;

ab = x(ab) + 0

para que isso seja possível, x deve ser igual a 1, nosso mdc

( ← )

Se o nosso mdc é igual a 1, pelo algoritmo euclidiano

ab = 1(ab) + 0

Então o mmc que multiplica nosso mdc deve ser o menor possível para gerar 1, sendo ele igual ao dividendo, ou seja igual ab também.

c. Para qualquer natural m, temos (a | m e b | m) sse mmc(a, b) | m.
(Dica: para a direção “⇒”, imagine a divisão euclidiana de m por mmc(a, b). O que de impossível teria que acontecer se o resto dessa divisão não fosse 0?)