Números Inteiros e Criptografia, PLE 2020, Lista de Exercícios 3
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049873

Questão 3. Sejam $n > m$ inteiros positivos. Mostre que se o resto da divisão de n por m é r, então o resto da divisão de $2 n - 1$ por $2 m - 1$ é $2 r - 1$. (Dica: a soma de uma progressão geométrica finita onde todos os termos são números naturais é um número natural!)

Questão 4. Sejam $n > m$ inteiros positivos. O objetivo desta questão é calcular mdc $((2^{2^n}) + 1, (2^{2^m}) + 1)$.
a. Usando que $(2^{2^{m+1}}) - 1 = ((2^{2^m}) + 1)((2^{2^m}) - 1)$, mostre que $(2^{2^n}) - 1$ é múltiplo de $(2^{2^m}) + 1$ quando $n > m$. Qual é o quociente desta divisão?

Questão 6. Encontre todos os inteiros positivos n tais que $2n\ 2 + 1 \mid n^3 + 9n - 17$.

> Temos que $n^3 + 9n - 17 = (2n^2 + 1)q + r$, da divisão de $n^3 + 9n - 17$ por $2n^2 + 1$ encontramos que q é igual a $n/2$ e resto $17n/2 - 17$, para que seja um divisão euclidiana o resto precisa ser igual a 0. Assim: $17n/2 - 17 = 0$, disso encontramos que o único n possível para encontrar resto 0 é $n=2$.

Questão 8. Verdadeiro ou falso? Apresente uma prova se a afirmação for verdadeira ou um contra-exemplo se ela for falsa.
a. O produto de dois números que deixam resto 7 quando divididos por 8 também deixa resto 7 quando dividido por 8.

> Sendo $a = bq + r$, temos que a é o dividendo, b é o divisor,q é o quociente e r é o resto
> Do enunciado tiramos que os números são:
> $X = 8q + 7$
> $Y = 8q' + 7$
>
> $X.Y = (8q + 7)*(8q' + 7) = 64qq' + 56q + 56q' + 49$
>
> Dessa multiplicação tiramos que $(64qq' + 56q + 56q')$ é múltiplo de 8 e 49 múltiplo de 7. Dessa forma não temos resto igual a zero quando dividimos $64qq' + 56q + 56q' + 49$ por 8, mas sim igual a 1. Sendo a afirmativa falsa.

Questão 11. Verdadeiro ou falso? Apresente uma prova se a afirmação for verdadeira ou um contra-exemplo se ela for falsa.

a. Sejam a, x e y inteiros. Se a divide $2x - 3y$ e a divide $4x - 5y$, então a divide y.

Do enunciado tiramos que:

$a|2x - 3y \wedge a|4x - 5y \rightarrow a|y$

Se 2x-3y é múltiplo de 'a', então qualquer número inteiro multiplicado por ele também é um múltiplo de 'a'. Assim $a|(2x - 3y) * 2$, escolhemos multiplicar por 2 para a prova final.

Como $a|2x - 3y \wedge a|4x - 5y$, então $a|(2x-3y) - (4x - 5)$, escolhendo a parte que foi multiplicada pelo inteiro (2) temos que;

$a|(2x-3y)*2 - (4x - 5y)$
$a|(4x-6y) - (4x-5y)$
$a|-y$
$a|y*(-1)$

Provando assim que $a|y$

b. Sejam a, b e c inteiros. Se b divide o produto ac, então b divide c

Contraexemplo:
$a = 6$
$c = 8$
$b = 12$

12 divide $6 . 8 = 48$, mas 12 não divide nem 6 e nem 8, portanto é falso.

c. Seja a um número inteiro. Se $a^2 - 2a + 7$ é par, então a é ímpar

Usando a contrapositiva: "Se 'a' não é ímpar, então '$a^2 - 2a + 7$' não é par"

Caso $a = 2$:

$a^2 - 2a + 7 = 7$

Provamos assim por contrapositiva que é verdade

Questão 13. Sejam a, b, c $\in$ N. Prove ou refute:

c. Se a | b e b | c, então a | c;

Temos:

a|b : b=aq

b|c : c=bq’, temos que b = c/q’

Temos então que:

c/q’ = aq

c = (aq)q’

Sendo q’ apenas mais um número multiplicando outro múltiplo de c, achamos que a|c.

d. Se a | b e a | c, então para todos x, y $\in$ Z temos a | (bx + cy);

a|b : b = aq

a|c : c = aq’

a | (bx + cy) : (bx + cy) = aq’’

(bx + cy) = ((aq)x+ (aq’)y)

Colocando o ‘a’ em evidência a((xq) + (yq’)) então ((xq) + (yq’)) pode ser q’’, logo a | (bx + cy)

e. Se a | b e b | a, então a = b;

b=aq ^ a=bq → bq = b

q=1

a = b

Provamos que é verdade

f . Se a | b então a ≤ b;

Temos que ‘a’ é um múltiplo de ‘b’ então:

b = aq

Caso q=1

a = b

Caso q>1

b>a

Então é verdadeiro

g. Se c =/= 0, então: a | b sse ac | bc (o que acontece no caso c = 0?);

Temos que a|b ←→ ac|bc

Sendo a um múltiplo de b, temos que:

a|b : b=aq

b=aq → ac|bc

Então:

$b=aq \rightarrow ac|(aq)c$

Temos agora que (ac) é um múltiplo de (aq)

$(aq)c = (ac)q'$

Por algebrismo chegamos que q'=q, como temos o mesmo quociente então está provado

Caso c=0:
$q.0=q'0$

Não temos como descobrir q e q'

Questão 16. Prove que para a, b, c $\in$ N, o mdc satisfaz as seguintes propriedades:
b. mdc(a, ca) = a.

Caso a >= ac:

Dividindo 'a' por 'ca' temos que o quociente para acharmos resto 0 igual a 1/c. Onde só pode ser c= 1, assim temos a=a, onde o divisor também é 'a'

Caso ac>=a:

Dividindo 'ca' por 'a', achamos resto 0 quanto o quociente é igual a 'c',que pelo Algoritmo de Euclides retornamos o divisor desta divisão como o mdc, sendo ele igual a 'a'

Provamos assim que mdc(a, ca) = a.