NÚMEROS INTEIROS E CRIPTOGRAFIA – UFRJ

GABARITO DA LISTA 0

Gabarito preparado por Leon Augusto (monitor 2012)

1. Contando o número de bs:

$$b^n \cdot b^m = \underbrace{b \cdots b}_{n \text{ vezes}} \cdot \underbrace{b \cdots b}_{m \text{ vezes}} = \underbrace{b \cdots b}_{m+n \text{ vezes}}$$

Vemos, assim, que esta potência é igual à base b elevada ao expoente que corresponde à soma $n + m$; donde a igualdade desejada.

2. Começamos abrindo a potência fora dos parênteses:

$$(b^m)^n = \underbrace{b^m \cdots b^m}_{n \text{ vezes}}$$

Usando o resultado anterior $n - 1$ vezes, obtemos

$$(b^m)^n = b^{2m} \cdot \underbrace{b^m \cdots b^m}_{n-2 \text{ vezes}} = b^{3m} \cdot \underbrace{b^m \cdots b^m}_{n-3 \text{ vezes}} = \cdots = b^{(n-1)m} \cdot b = (b^m)^n.$$

3. Pela igualdade do exercício 2:

$$(b^{k^m})^{k^n} = b^{k^m + k^n}.$$

Mas, pela igualdade do exercício 1:

$$k^m + k^n = k^{m+n}.$$

Combinando as duas, obtemos

$$(b^{k^m})^{k^n} = b^{k^m + k^n} = b^{k^{m+n}}.$$

4. Usando o que aprendemos nos dois exercícios anteriores:

   (a) $2^5 \cdot 3^5 = (2 \cdot 3)^5 = 6^5$;
   (b) $(2^5)^6 \cdot 2^7 = 2^{30} \cdot 2^7 = 2^{37}$;
   (c) $(2^{3^4})^{3^9} = 2^{3^{13}}$;
   (d) $(2^{3^4})^{5^4} = 2^{3^4 \cdot 5^4} = 2^{15^4}$.

5. Usando o que aprendemos nos exercícios 1 e 2:

$$(3^{2^8})^{2^5} \cdot (3^{2^6})^{2^7} = 3^{2^{8+5}+2^{6+7}} = 3^{2\cdot 2^{13}} = 3^{2^{14}}.$$

6. Multiplicando o lado esquerdo da igualdade, obtemos

$$(x^2 - ny^2)(u^2 - nv^2) = x^2u^2 - x^2 \cdot nv^2 - ny^2 \cdot u^2 + n^2y^2v^2,$$

que, rearrumando, nos dá

$$(x^2 - ny^2)(u^2 - nv^2) = (xu)^2 - n \cdot (xv)^2 - n(yu)^2 + (nyv)^2. \tag{1}$$

Por outro lado, expandindo o lado direito da primeira igualdade:

$(xu + nyv)^2 - n(xv + yu)^2 = ((xu)^2 + 2nxuyv + (nyv)^2) - n((xv)^2 + 2xvyu + (yu)^2)$;

donde

$(xu + nyv)^2 - n(xv + yu)^2 = ((xu)^2 + 2nxuyv + (nyv)^2) - (n(xv)^2 + 2nxvyu + n(yu)^2)$.

Cancelando a parcela $2nxvyu$, resta:

$$(xu + nyv)^2 - n(xv + yu)^2 = ((xu)^2 + (nyv)^2) - n((xv)^2 + (yu)^2).$$

Comparando com (1), vemos que

$(xu + nyv)^2 - n(xv + yu)^2 = ((xu)^2 + (nyv)^2) - n((xv)^2 + (yu)^2) = (x^2 - ny^2)(u^2 - nv^2)$,

provando a igualdade desejada. A outra identidade é provada de maneira semelhante.