LISTA 8 - GABRIEL ALMEIDA MENDES

(1) CALCULE A FORMA REDUZIDA DE CADA ITEM ABAIXO:

h) $2^{130} \pmod{263}$ (USE O FATO QUE $2^{131} \equiv 1 \pmod{263}$)

$R: 2^{131-1} \pmod{263}$

$2^{131} : 2^1 \pmod{263}$

$1 : 2^1 \bmod 263$

$\frac{1}{2} \bmod 263$

$\frac{1}{2} = 263q + r$

$r = \frac{1}{2} \quad q = 0$

$a \equiv r$

$\frac{1}{2} \bmod 263$

(3) DETERMINE O RESTO DA DIVISÃO

e) $39^{50!}$ Por 2251 (USE O FATO QUE $39^{1125} \equiv 1 \pmod{2251}$)

$39^{50 \cdot 49 \cdot \ldots \cdot 2 \cdot 1}$ Por 2251

$39^{1125} \equiv 1 \bmod 2251$

$(39^{25 \cdot 45})^{1 \cdot \ldots \cdot 24 \cdot 26 \cdot \ldots \cdot 44 \cdot 46 \cdot \ldots \cdot 50}$

$(1)^{1 \cdot \ldots \cdot 24 \cdot 26 \cdot \ldots \cdot 44 \cdot 46 \cdot \ldots \cdot 50}$

$39^{50!} \equiv 1 \bmod 2251$

1125	3
375	3
125	5
25	5
5	5
1	

$3^2 \cdot 5^3$

$3 \cdot 3 \cdot 5 \quad 5 \cdot 5$

$45 \quad 25$

g) $2^{987657} + 5^{15}$ Por 65 (DICA: $2^6 \equiv 64 \equiv -1 \pmod{65}$)

$2^{6 \cdot 164609 + 3} + 5^{15}$

$(2^6)^{164609} \cdot 2^3 + (5^5)^3$

$(-1) \cdot 2^3 + (5)^3$

$-8 + 60$

$52 \bmod 65$

$5^n \equiv 1 \bmod 65$

$5 - n = 65q$

$n = 5 \quad q = 0$

$5^5 \equiv 5$

(4) PROVE POR INDUÇÃO QUE $\forall m \in \mathbb{N}, m \geq 1$, TEMOS $m^3 \equiv m \pmod 6$

$m^3 \equiv m \pmod 6$

$m^6 \equiv m^2 \pmod 6$

CASO BASE ($m = 0$)

$0 \equiv 0 \pmod 6$

$0^p \equiv 0 \pmod p$

$Q(0)$

CASO INDUTIVO ($p = 6$)

$Q(a)$

$m^6 \equiv m^2 \pmod 6$

$m^6 + 1 \equiv m^2 + 1 \pmod 6$

$m^6 + \overbrace{6m^5 + 15m^4 + 20m^3 + 15m^2 + 6m}^{=0} + 1 \equiv m^2 + 1 \pmod 6$

$(m+1)^6 \equiv m^2 + 1 \pmod 6$

$(m+1)^3 \equiv m + 1 \pmod 6$

$Q(a+1)$

(9) $p > 1200$ É UM FATOR PRIMO DE $1200! + 1$. $\overline{1200}$ TEM INVERSO EM $\mathbb{Z}_p$? SE EXISTIR, QUAL É O SEU INVERSO EM $\mathbb{Z}_p$

RESPOSTA:

COMO p É FATOR DE $1200! + 1$, ENTÃO $1200! + 1 \equiv 0 \pmod p$, DE MODO QUE $1200! \equiv -1 \pmod p$.

ASSIM, $1200(-(1199!)) \equiv 1 \pmod p$.

LOGO $\overline{1200}$ TEM INVERSO EM $\mathbb{Z}_p$ E SEU INVERSO É $-(1199!)$.

(13) a) COMO 6 NÃO É DIVISÍVEL POR 7 E O MESMO É PRIMO, PELO TEOREMA DE FERMAT PODEMOS USAR $6^6 \equiv 1 \pmod 7$. POIS NOTA-SE QUE OS EXPOENTES DOS TERMOS SÃO FATORIAIS E, QUANDO A BASE DO FATORIAL É MAIOR OU IGUAL DO QUE 3, O EXPOENTE FICA MÚLTIPLO DE 6

b) PODEMOS USAR O TEOREMA NO CÁLCULO, CALCULANDO A CONGRUÊNCIA DE CADA TERMO E DEPOIS SOMANDO.

$1 \equiv 1 \pmod 7$

$2^{2!} \equiv 4 \pmod 7$

$3^{3!} \equiv 1 \pmod 7$

$4^{4!} \equiv 1 \pmod 7$

$5^{5!} \equiv 1 \pmod 7$

$6^{6!} \equiv 1 \pmod 7$

$7^{7!} \equiv 7 \equiv 0 \pmod 7$

$8^{8!} \equiv 1 \pmod 7$

$9^{9!} \equiv 1 \pmod 7$

$10^{10!} \equiv 1 \pmod 7$

$\equiv 1 + 4 + 1 + 1 + 1 + 1 + 0 + 1 + 1 + 1 \pmod 7$

$\equiv 12 \pmod 7$

$\equiv 5 \pmod 7$

(15) DETERMINE SE AS RELAÇÕES SÃO REFLEXIVAS, SIMÉTRICAS E/OU TRANSITIVAS. ALGUMA DAS DUAS RELAÇÕES É DE EQUIVALÊNCIA?

(1) aR_1b QUANDO $MDC(a,b)=1$.

(2) FIXE $m>0$ INTEIRO. ENTÃO aR_2b QUANDO $mdc(a,m)=mdc(b,m)$

(1)

- REFLEXIVA

$\forall a,b \in X \quad aRa \in bRb$ A RELAÇÃO NÃO REFLEXIVA POIS O NUMEROS SÃO PRIMOS ENTRE SI

- SIMETRICA

$\forall a,b \in X \quad aRb \rightarrow bRa$, A RELAÇÃO É SIMETRICA

- TRANSITIVA

$\forall a,b \in X \quad aRb \in bRy$, A RELAÇÃO NÃO É TRANSITIVA

- NÃO É UMA RELAÇÃO DE EQUIVALÊNCIA

(2)

- REFLEXINA

$\forall a,b \in x \quad aRa \in bRb$, A RELAÇÃO É REFLEXIVA

- SIMETRICA

$\forall a,b \in x \quad aRb \rightarrow bRa$, A RELAÇÃO É SIMETRICA

- TRANSITIVA

$\forall a,b,m \in x \quad aRm \in mRb \Rightarrow aRb$, A RELAÇÃO É TRANSITIVA

- É UMA RELAÇÃO DE EQUIVALÊNCIA

OBS: ÉU NÃO SOUBE COMO TRANSPOR EM PALAVRAS MINHAS CONCLUSÕES, POIS EU USEI MAIS MINHA INTUIÇÃO PARA RESPONDÊ-LAS.

19) OBJETIVO: MOSTRAR QUE NENHUM NÚMERO DA FORMA $4m+3$ PODE SER ESCRITO COMO A SOMA DOS QUADRADOS DE DOIS INTEIROS.

a) MOSTRE QUE O QUADRADO DE QUALQUER INTEIRO SÓ PODE SER CONGRUENTE A 0 OU 1 MÓDULO 4.

RESPOSTA:

SE O NÚMERO É PAR ENTÃO É DA FORMA $2k$, MAS $(2k)^2 \equiv 4k^2 \equiv 0 \mod 4$.
SE O NÚMERO É IMPAR ENTÃO É DA FORMA $2k+1$, DONDE $(2k+1)^2 \equiv 4(k^2+k)+1 \equiv 1 \mod 4$.

b) MOSTRE QUE SE $x \in y \in \mathbb{Z}$ ENTÃO x^2+y^2 SÓ PODE SER CONGRUENTE A 0, 1 OU 2 MÓDULO 4.

RESPOSTA:

SEJAM x E y INTEIROS, ENTÃO x^2 E y^2 SÓ PODEM SER CONGRUENTES A 0 OU 1 MÓDULO 4 PELA QUESTÃO 19.a. PODEMOS CONSTRUIR A SEGUINTE TABELA:

x	y	x^2+y^2
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{0}$	$\bar{1}$	$\bar{1}$
$\bar{1}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{2}$

LOGO x^2+y^2 PODE SER CONGRUENTE SOMENTE A 0, 1 OU 2 MÓDULO 4.

c) MOSTRE QUE UM INTEIRO DA FORMA $4m+3$ NÃO PODE SER CONSTRUÍDO COMO A SOMA DE DOIS QUADRADOS DE INTEIROS

RESPOSTA

SE EXISTISSEM INTEIROS x E y TAIS QUE $x^2+y^2=4m+3$ ENTÃO TERÍAMOS $x^2+y^2 \equiv 3 \mod 4$ O QUE NÃO É VERDADE COMO VIMOS PELA QUESTÃO 19.b.