Números Inteiros e Criptografia — Prova Final (segunda chamada, parte 1)
9/7/2019

A prova é individual e sem consulta. Responda as questões na folha de respostas, a lápis ou a caneta. Se tiver qualquer dúvida consulte o professor. Você pode usar livremente qualquer resultado visto em sala ou em listas de exercício, mas deve escrever claramente qual é o teorema/exercício/fato sendo usado. É **proibido** o uso de celular.

JUSTIFIQUE SUAS RESPOSTAS!

Questão 1. (1½ pontos) Uma loja de informática vende mouses a R$ 35 cada, teclados a R$ 72 cada, e computadores a R$ 2520 cada. Um cliente entra na loja com uma certa quantia na carteira. Se ele gastar o máximo possível comprando mouses, ele receberá R$ 18 de troco, mas se gastar o máximo possivel comprando teclados, receberá R$ 51 de troco. Quanto ele receberá de troco se em vez de mouses ou teclados, ele decidir comprar o máximo de computadores possível?

Questão 2. (1½ pontos) Mostre que $1+8+27+64+125+\cdots+n^3 = \dfrac{n^2(n+1)^2}{4}$ é verdadeiro para todo inteiro $n \geq 1$.

Questão 3. (1 ponto) Como vimos, se p é primo, então para quaisquer inteiros positivos a e b, temos: p divide $a \cdot b$ sse p divide a ou p divide b (ou ambos). Mostre que a recíproca é verdadeira: **se** p é um inteiro positivo tal que para todos inteiros positivos a e b temos que p divide $a \cdot b$ sse p divide a ou p divide b (ou ambos), **então** p é primo.

Questão 4. Diga quais dos números abaixos possuem inverso multiplicativo no universo indicado. Nos casos positivos, diga quem é o inverso; nos negativos, diga porque o número não tem inverso.

(a) (½ ponto) $\overline{25}$ em $\mathbb{Z}_{32}$.

(b) (½ ponto) -1 em $\mathbb{Z}$.

(c) (½ ponto) 2 em $\mathbb{Z}$.

Números Inteiros e Criptografia — Prova Final (segunda chamada, parte 2)
11/7/2019

A prova é individual e sem consulta. Responda as questões na folha de respostas, a lápis ou a caneta. Se tiver qualquer dúvida consulte o professor. Você pode usar livremente qualquer resultado visto em sala ou em listas de exercício, mas deve escrever claramente qual é o teorema/exercício/fato sendo usado. É **proibido** o uso de celular.

JUSTIFIQUE SUAS RESPOSTAS!

Questão 5. Encontre a forma reduzida de:

(a) (½ ponto) $12345523423657^{19239} \pmod 5$

(b) (½ ponto) $3577714496370917^{123456789123456789123456789} \pmod 7$

Questão 6. Para esta questão, use a codificação de símbolos da tabela abaixo.

código	*símb.*
11	0
12	1
13	2
14	3
15	4
16	5
17	6
18	7
19	8
21	9
22	.
23	,
24	!

código	*símb.*
25	?
26	:
27	;
28	"
29	(
31	)
32	+
33	-
34	*
35	/
36	=
37	_
38	A

código	*símb.*
39	B
41	C
42	D
43	E
44	F
45	G
46	H
47	I
48	J
49	K
51	L
52	M
53	N

código	*símb.*
54	O
55	P
56	Q
57	R
58	S
59	T
61	U
62	V
63	W
64	X
65	Y
66	Z
67	À

código	*símb.*
68	Á
69	Â
71	Ã
72	É
73	Ê
74	Í
75	Ó
76	Ô
77	Õ
78	Ú
79	(espaço)

Você e mais dois usuários, Alice e Bob, resolvem se comunicar usando RSA, de acordo com a codificação de símbolos da tabela acima e usando as chaves da tabela abaixo:

Usuário	**Chave pública**	**Chave privada**
Você	(905, 4661)	(5, 4661)
Alice	(3, 6319)	?
Bob	(5, 7081)	?

(a) (1 ponto) Em um certo momento, você recebe quatro blocos encriptados, vindos da Alice: `1637, 931, 1751, 3216`. Qual é a mensagem descriptada?

(b) (1 ponto) Envie alguma mensagem encriptada para o Bob.

A prova continua no verso!

Questão 7. Para cada número abaixo, diga se ele é composto ou *provavelmente* primo, **usando os testes de Fermat e/ou Miller–Rabin**. Caso o teste usado seja inconclusivo, você deve também utilizar o outro teste.

(a) (½ ponto) 2701

(b) (½ ponto) 2047

(c) (½ ponto) 2003

Questão 8. (1 ponto) Seja $(G, *)$ um grupo e suponha que, para **todo** $a \in G$ tenhamos $a^2 = e$. Mostre que o grupo $(G, *)$ é abeliano, i.e., que para todos $a, b \in G$ temos

$$a * b = b * a.$$

Dica: dados $a, b \in G$, considere o elemento $(a * b)^2$.