Números Inteiros e Criptografia 2019.2 — Segunda prova — 5/11/2019

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. Para esta questão, considere a correspondência entre caracteres e números indicados na Tabela 1 (no verso) e suponha que queiramos usar a *cifra multiplicativa* com chave de encriptação e, na qual o caracter correspondente ao número C é transformado no caracter correspondente ao número $C \cdot e \pmod N$, sendo N a quantidade de caracteres que estamos considerando no alfabeto (no nosso caso, $N = 100$).

(a) (1 ponto) Uma chave de *descriptação* d correspondente a e é um número inteiro com a propriedade

$$C \cdot e \cdot d \equiv C \pmod N$$

para qualquer inteiro C. Diga como d pode ser obtido a partir de e & N.

(b) ($1\frac{1}{2}$ pontos) Sabendo que a mensagem a seguir foi encriptada usando a chave $e = 91$, diga qual era a mensagem original.

oÓ:HjsrÓô;ZôÓZ

Questão 2. (3 pontos) Calcule a forma reduzida de $601^{\left(7^{8713}\right)} \pmod{599}$.

Questão 3. ($2\frac{1}{2}$ pontos) Mostre que para todo inteiro b temos $b^{75361} \equiv b \pmod{75361}$.
Dica: 75361 **não é** primo!

Questão 4. (a) ($1\frac{1}{2}$ pontos) Mostre que se n é composto então $(n-1)! \equiv 0 \pmod n$.

(b) ($1\frac{1}{2}$ pontos) Use o item (a) para criar um teste (correto) que receba como entrada um número n e responda "n é primo" ou "teste inconclusivo". Você não precisa provar a terminação nem a corretude do seu teste.

código	*caracter*
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	a
11	b
12	c
13	d
14	e
15	f
16	g
17	h
18	i
19	j
20	k
21	l
22	m
23	n
24	o

código	*caracter*
25	p
26	q
27	r
28	s
29	t
30	u
31	v
32	w
33	x
34	y
35	z
36	à
37	á
38	â
39	ã
40	ç
41	é
42	ê
43	í
44	ó
45	ô
46	õ
47	ú
48	A
49	B

código	*caracter*
50	C
51	D
52	E
53	F
54	G
55	H
56	I
57	J
58	K
59	L
60	M
61	N
62	O
63	P
64	Q
65	R
66	S
67	T
68	U
69	V
70	W
71	X
72	Y
73	Z
74	À

código	*caracter*
75	Á
76	Â
77	Ã
78	Ç
79	É
80	Ê
81	Í
82	Ó
83	Ô
84	Õ
85	Ú
86	.
87	,
88	!
89	?
90	:
91	;
92	"
93	+
94	-
95	*
96	/
97	=
98	§
99	(espaço)

Tabela 1: Codificação de caracteres para a **Questão 1**.