Números Inteiros e Criptografia — Primeira prova (parte 1) — 13/5/2019

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 e suponha que queiramos usar a *cifra multiplicativa* com chave 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) Para quantas chaves de encriptação e com $1 \leq e < 100$ existe uma chave de *descriptação* d correspondente? Qual é a propriedade que deve valer entre e & d para que d seja a chave de descriptação correspondente à chave de encriptação e, e por quê?

(b) ($\frac{1}{2}$ ponto) Como você pode obter d a partir de e?

(c) ($\frac{1}{2}$ ponto) Imagine que um amigo tenha te passado um bilhete de cola durante a prova com a seguinte mensagem encriptada:

ÀÍo?4:yTLZ3DyíMêê3Ã

Sabendo que a mensagem original foi encriptada usando a chave 91, diga qual é a mensagem descriptada.

Questão 2. Imagine uma espécie de seres alienígenas com as seguintes características:

- Os seres dessa espécie são imortais;
- Cada ser dessa espécie se torna maduro para poder se reproduzir exatamente quando completa 1 ano de vida;
- Os seres dessa espécie se reproduzem assexuadamente, e cada ser começa a se reproduzir exatamente no momento em que se torna maduro, ou exatamente no momento em que acabou de se reproduzir mais recentemente;
- Cada processo de reprodução demora exatamente 1 ano entre seu início e seu final, e cada processo de reprodução individual gera 1 novo ser.

(a) (1 ponto) Suponha que uma população desses seres comece vazia no instante atual e receba magicamente um ser recém-nascido dessa espécie daqui a exatamente 1 ano. Sendo $A(n)$ a quantidade de seres dessa população daqui a n anos, escreva uma relação de recorrência para $A(n)$, i.e., uma fórmula que expresse o valor de $A(n)$ diretamente em alguns casos, e que nos demais casos permita calcular o valor de $A(n)$ *assumindo que sabemos* os valores de $A(m)$ para $m < n$.

(b) (1 ponto) Prove que, se daqui a n anos o tamanho da população é um número múltiplo de 5, então isso acontece novamente daqui a $n + 5$ anos.

(c) (1 ponto) Sejam m e k inteiros positivos tais que $m > k$ e $1 + \frac{k}{m} < \frac{m}{k}$. Prove que $A(n) < (\frac{m}{k})^n$ para todo $n \geq 1$ (dica: use *indução forte*: "para provar que uma certa propriedade é válida para todo natural $n \geq n_0$, prove que:

- ela é válida para n_0
- para qualquer $n > n_0$:
  se ela é válida para todo natural m com $n_0 \leq m < n$, **então** ela é válida para n".

Questão 3. Sejam p um número primo e a um número natural.

(a) (½ ponto) Quais são os possíveis restos da divisão de a^{p-1} por p?

(b) (½ ponto) Se você escolhe um número natural a aleatoriamente (nenhum número é mais provável de ser sorteado do que nenhum outro), qual a probabilidade aproximada de se obter cada um dos restos possíveis da divisão de a^{p-1} por p?

código	*caracter*
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	.
11	,
12	!
13	?
14	:
15	;
16	"
17	(
18	)
19	+
20	-
21	*
22	/
23	=
24	_

código	*caracter*
25	a
26	b
27	c
28	d
29	e
30	f
31	g
32	h
33	i
34	j
35	k
36	l
37	m
38	n
39	o
40	p
41	q
42	r
43	s
44	t
45	u
46	v
47	w
48	x
49	y

código	*caracter*
50	z
51	à
52	á
53	â
54	ã
55	ç
56	é
57	ê
58	í
59	ó
60	ô
61	õ
62	ú
63	A
64	B
65	C
66	D
67	E
68	F
69	G
70	H
71	I
72	J
73	K
74	L

código	*caracter*
75	M
76	N
77	O
78	P
79	Q
80	R
81	S
82	T
83	U
84	V
85	W
86	X
87	Y
88	Z
89	À
90	Á
91	Â
92	Ã
93	É
94	Ê
95	Í
96	Ó
97	Ô
98	Õ
99	Ú

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

Números Inteiros e Criptografia — Primeira prova (parte 2) — 14/5/2019

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 4. Como vimos, há diversos *truques* para calcular potências em aritmética modular, cada um aplicável em uma situação diferente. Vamos agora desenvolver uma técnica rápida que funciona em geral, e é de fato implementada, por exemplo, na função `pow` do Python.

Sejam a, e, n números inteiros positivos e suponha que você queira calcular a forma reduzida de a^e módulo n, i.e., encontrar o menor natural r tal que $a^e \equiv r \pmod{n}$. Sabendo que a representação binária de e é $(b_m b_{m-1} b_{m-2} \cdots b_1 b_0)_2$, i.e., que $b_0, b_1 \ldots, b_m$ são naturais menores que 2 e

$$e = \sum_{i=0}^{m} b_i \cdot 2^i = b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + \cdots + b_m \cdot 2^m,$$

temos

$$a^e \equiv \prod_{i=0}^{m} a^{b_i \cdot (2^i)} \equiv \prod_{i=0}^{m} (a^{(2^i)})^{b_i} \pmod{n}. \qquad (*)$$

Portanto, o problema é calcular a forma reduzida do produto $(*)$ módulo n.

(a) (1 ½ pontos) Descreva um algoritmo para encontrar a forma reduzida de a^e módulo n, usando apenas as seguintes operações auxiliares:

1. encontrar a representação binária de um natural qualquer;
2. encontrar a forma reduzida de um natural qualquer módulo n;
3. elevar ao quadrado um natural menor do que n;
4. multiplicar dois naturais menores do que n.

Você **não precisa** descrever algoritmos para realizar essas operações auxiliares!

Dica: Você vai calcular o produto $(*)$ passo-a-passo; na hora de calcular a forma reduzida de $a^{(2^{i+1})}$ módulo n, use o fato de que você calculou a forma reduzida de $a^{(2^i)}$ módulo n no passo anterior! Feito isso, o expoente b_{i+1} (que é 0 ou 1) indica se você deve multiplicar o número resultante com o seu *produto parcial* encontrado até agora ou não.

(b) (½ ponto) Utilize o seu algoritmo para calcular a forma reduzida de 13^{75} módulo 9; mostre o passo-a-passo da execução.

Dica: $75 = (1001011)_2$.

Questão 5. Sejam a, b, c, n inteiros positivos.

(a) (1 ponto) Mostre que, se

$$b^a \equiv 1 \pmod{n} \qquad \text{e} \qquad b^c \equiv 1 \pmod{n},$$

então

$$b^{\mathrm{mdc}(a,c)} \equiv 1 \pmod{n}.$$

Dica: Há uma fórmula que expressa $\mathrm{mdc}(a, c)$ usando a e c.

(b) (1 ponto) Mostre que, se p é primo e $b^n \equiv 1 \pmod{p}$, então:

- existe algum divisor d de n, *diferente* de n, tal que $b^d \equiv 1 \pmod{p}$

ou

- $p \equiv 1 \pmod{n}$. Neste caso, se $p > 2$ e n é ímpar, mostre também que $p \equiv 1 \pmod{2n}$.

Dica: Mostre que existe algum m com $b^m \equiv 1 \pmod{p}$ e use a parte (a).

(c) (1 ponto) Seja $N = 2^{17} - 1 = 131071$. Há 72 primos menores do que $\sqrt{N}$, e a Tabela 2 mostra os restos das divisões destes primos por $2 \cdot 17 = 34$. Mostre que N é primo.

Dica: Para cada primo $p < \sqrt{N}$, queremos saber se p divide N. Use o fato de que 17 é primo e a contrapositiva da parte (b) da questão para concluir que a *grande maioria* dos primos $p < \sqrt{N}$ não divide N; para os poucos restantes, faça a conta.

r	primos $p < \sqrt{N}$ com $p \equiv r \pmod{34}$
1	103, 137, 239, 307
2	2
3	3, 37, 71, 139, 173, 241
5	5, 73, 107, 277, 311
7	7, 41, 109, 211, 313, 347
9	43, 179, 281, 349
11	11, 79, 113, 181, 283, 317
13	13, 47, 149, 251, 353
15	83, 151

r	primos $p < \sqrt{N}$ com $p \equiv r \pmod{34}$
17	17
19	19, 53, 223, 257, 359
21	89, 157, 191, 293
23	23, 193, 227
25	59, 127, 229, 263, 331
27	61, 163, 197
29	29, 97, 131, 199, 233
31	31, 167, 269, 337
33	67, 101, 271

Tabela 2: **Questão 5**.