INSTITUTO DE COMPUTAÇÃO

Universidade Federal do Rio de Janeiro
Centro de Ciências Matemáticas e da Natureza

Números Inteiros e Criptografia 2023.1

Prova 1 — 15 de junho de 2023

Justifique todas as suas respostas!
Você pode usar tudo que foi feito em sala ou em listas de exercícios, devendo apenas ser claro quando fizer isso. Você também pode usar qualquer questão da prova na solução de outra, desde que não crie dependências circulares.

Questão 1. Existem múltiplos inteiros de 7575 e 3342 cuja soma seja -32? Se sim, encontre-os; se não, prove que não existem.

Questão 2. Considere a seguinte função $\ell : \mathbb{N} \to \mathbb{N}$, conhecida como *função de Liouville*:

$$\ell(n) = \begin{cases} n, & \text{se } n \leqslant 1 \\ 1, & \text{se } n \geqslant 2 \text{ e } n \text{ tem uma quantidade par de fatores primos} \\ & \text{no total, i.e., contando todas as repetições} \\ -1, & \text{nos outros casos.} \end{cases}$$

Assim, temos $\ell(6) = \ell(2 \cdot 3) = 1$ e $\ell(12) = \ell(2 \cdot 2 \cdot 3) = -1$, por exemplo.

Prove que ℓ é uma função completamente multiplicativa, ou seja, prove que para todos naturais n, m temos

$$\ell(n \cdot m) = \ell(n) \cdot \ell(m).$$

Questão 3. Prove que $2^{4194303} - 1$ não é um número primo. Para ajudar, as tabelas abaixo trazem as primeiras 25 potências de 2.

i	2^i	i	2^i	i	2^i	i	2^i	i	2^i
0	1	5	32	10	1024	15	32768	20	1048576
1	2	6	64	11	2048	16	65536	21	2097152
2	4	7	128	12	4096	17	131072	22	4194304
3	8	8	256	13	8192	18	262144	23	8388608
4	16	9	512	14	16384	19	524288	24	16777216

Questão 4. Nesta questão, considere a seguinte correspondência entre **21** símbolos e números:

cód.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
símb.	a	b	c	d	e	g	h	i	l	m	n	o	p	q	r	s	t	u	,	?	_

a. Dos números de 2 até 20 (inclusive), quais chaves podem ser usadas para encriptar mensagens usando cifra multiplicativa nesse sistema? Lembre-se de justificar a sua resposta. Sua resposta não pode ser baseada na tabela abaixo.

b. Você descobriu que o seu amigo envia mensagens em cifra multiplicativa com a correspondência acima, usando chave de encriptação 16. Novamente sem usar a tabela abaixo, e sem ser por tentativa e erro, descubra a chave de descriptação desse seu amigo.

c. Você interceptou uma mensagem que esse seu mesmo amigo enviou para alguém: `tcagtcbgtci`
Usando a chave de descriptação descoberta no item anterior, desvende a mensagem original.

Para facilitar seu trabalho, você pode usar a tabela abaixo. Nela, cada célula indica a "casa do ciclo" resultante de se partir de algum número na "casa do ciclo" indicada pela linha e multiplicar pelo número indicado na coluna. Por exemplo, partindo de qualquer número na casa do `m` e multiplicando por `10`, chega-se à casa do `h`, e partindo de qualquer número na casa do `c` e multiplicando por `17`, chega-se à casa do `q`.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
b	a	b	c	d	e	g	h	i	l	m	n	o	p	q	r	s	t	u	,	?	_
c	a	c	e	h	l	n	p	r	t	,	_	b	d	g	i	m	o	q	s	u	?
d	a	d	h	m	p	s	,	a	d	h	m	p	s	,	a	d	h	m	p	s	,
e	a	e	l	p	t	_	d	i	o	s	?	c	h	n	r	,	b	g	m	q	u
g	a	g	n	s	_	e	m	r	?	d	l	q	,	c	i	p	u	b	h	o	t
h	a	h	p	,	d	m	s	a	h	p	,	d	m	s	a	h	p	,	d	m	s
i	a	i	r	a	i	r	a	i	r	a	i	r	a	i	r	a	i	r	a	i	r
l	a	l	t	d	o	?	h	r	b	m	u	e	p	_	i	s	c	n	,	g	q
m	a	m	,	h	s	d	p	a	m	,	h	s	d	p	a	m	,	h	s	d	p
n	a	n	_	m	?	l	,	i	u	h	t	g	s	e	r	d	q	c	p	b	o
o	a	o	b	p	c	q	d	r	e	s	g	t	h	u	i	,	l	?	m	_	n
p	a	p	d	s	h	,	m	a	p	d	s	h	,	m	a	p	d	s	h	,	m
q	a	q	g	,	n	c	s	i	_	p	e	u	m	b	r	h	?	o	d	t	l
r	a	r	i	a	r	i	a	r	i	a	r	i	a	r	i	a	r	i	a	r	i
s	a	s	m	d	,	p	h	a	s	m	d	,	p	h	a	s	m	d	,	p	h
t	a	t	o	h	b	u	p	i	c	,	q	l	d	?	r	m	e	_	s	n	g
u	a	u	q	m	g	b	,	r	n	h	c	?	s	o	i	d	_	t	p	l	e
,	a	,	s	p	m	h	d	a	,	s	p	m	h	d	a	,	s	p	m	h	d
?	a	?	u	s	q	o	m	i	g	d	b	_	,	t	r	p	n	l	h	e	c
_	a	_	?	,	u	t	s	r	q	p	o	n	m	l	i	h	g	e	d	c	b