INSTITUTO DE COMPUTAÇÃO

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

Números Inteiros e Criptografia 2022.1[†]

Prova 1

23 de junho de 2022

Justifique todas as suas respostas.

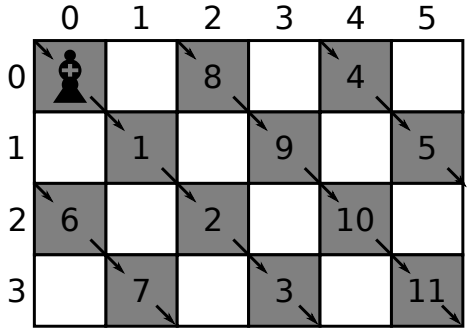
Questão 1 (3 pontos)**.** Os *números primos de Mersenne* são os números primos da forma $2^m - 1$ para algum natural m. Por exemplo, $3 = 2^2 - 1$ e $31 = 2^5 - 1$ são primos de Mersenne, mas 13 não é de Mersenne apesar de ser primo.

Prove que se $2^m - 1$ é um primo de Mersenne, então m é um primo (não necessariamente de Mersenne).

Dica: se você quiser, você pode usar (sem provar) que para qualquer natural $n > 0$ e quaisquer reais x, y temos

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + x^2y^{n-3} + xy^{n-2} + y^{n-1})$$

Questão 2. Em um tabuleiro de xadrez, mas com n linhas e m colunas (sendo n, m naturais e $n, m \geq 2$), um bispo é colocado na casa da ponta superior esquerda. Como no xadrez comum, o bispo pode se mover apenas nas diagonais, mas uma quantidade arbitrária de casas a cada movimento. Entretanto, temos um detalhe adicional: quando ele chega na borda do tabuleiro, ele pode continuar se movendo, "dando a volta" pela borda oposta (como em um jogo tipo *Pac-Man*). Veja a figura abaixo para um exemplo com $n = 4$ e $m = 6$, mostrando os movimentos possíveis do bispo (os números dentro das casas indicam a sequência das casas visitadas no movimento; os números fora do tabuleiro indicam as linhas e colunas, contando a partir de 0 como de costume).



a (1 ponto)**.** Complete as frases a seguir e dê argumentos que justifiquem as frases resultantes:

"Para todos p, ℓ naturais: após um movimento passando por p casas, o bispo está na linha ℓ do tabuleiro sse ..."

"Para todos p, c naturais: após um movimento passando por p casas, o bispo está na coluna c do tabuleiro sse ..."

[†]Como sempre, você pode usar tudo que foi visto em sala ou nas listas de exercícios, desde que cite claramente que está usando algo já visto. Você também pode citar uma questão da prova para resolver outra, desde que isso não introduza dependências circulares. Se você citar uma questão que não resolveu, receberá apenas uma pontuação parcial.

b (2 pontos)**.** Complete a frase a seguir e dê um argumento que justifique a frase resultante:

"Para todo p natural: após um movimento passando por p casas, o bispo está pela primeira vez de volta à sua posição original sse ..."

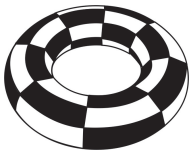
c (2 pontos)**.** Agora imagine que, com o bispo em sua casa original no canto superior esquerdo, uma outra peça de xadrez é colocada no tabuleiro. Complete a frase a seguir e dê um argumento que justifique a frase resultante:

"O bispo consegue atacar a outra peça (qualquer que seja sua posição) em um único movimento sse ...". *Dica.* Repare que no tabuleiro 4×6 da figura existem várias casas que o bispo não consegue atacar.

Dica/lembrete geral para essa questão. Dados naturais $a, b > 0$, definimos o $\text{mmc}(a, b)$ como o menor natural positivo que é múltiplo de ambos a e b. Você pode usar o seguinte fato (que provamos em uma aula de exercícios):

$$ab = \text{mmc}(a, b) \cdot \text{mdc}(a, b).$$

Curiosidade: os matemáticos imaginariam que esse tabuleiro não está em uma folha plana, mas sim que a folha foi "enrolada" e as bordas coladas, formando um cilindro, e que depois o cilindro em si foi enrolado e suas pontas coladas, formando uma "rosquinha". A figura resultante é chamada *toro*, então essa questão poderia ter como título "movimentos do bispo no xadrez jogado no toro".



Questão 3 (3 pontos)**.** Nesta questão vamos usar a correspondência entre 30 símbolos e números das tabelas abaixo. Escolha uma chave de encriptação válida para a cifra multiplicativa (não escolha a chave 1), me informe a chave escolhida, diga qual a chave de descriptação correspondente e me envie uma mensagem encriptada. A mensagem pode ser bem curta (mas deve ser inteligível)!

símbolo	a	b	c	d	e	f	g	h	i	j
número	0	1	2	3	4	5	6	7	8	9

símbolo	k	l	m	n	o	p	q	r	s	t
número	10	11	12	13	14	15	16	17	18	19

símbolo	u	v	w	x	y	z	,	!	?	(espaço em branco)
número	20	21	22	23	24	25	26	27	28	29

Boa prova!