Números Inteiros e Criptografia
2015/2

Prof. Luís Menasché Schechter

Observações:

1) *Não são aceitas respostas sem justificativa.* O aluno deve saber explicar tudo o que fizer.
2) Leia com atenção os enunciados até o final antes de começar a escrever as respostas.
3) A prova deve ser toda feita a caneta azul ou preta.

Questão 1: *(4 pontos)*

a) Determine os elementos do grupo $U(24)$ com a operação de multiplicação modular. *(0.5 ponto)*

b) Qual é a ordem deste grupo? Quais são as possíveis ordens dos subgrupos deste grupo? Justifique sua resposta! *(0.5 ponto)*

c) Determine todos os subgrupos cíclicos de $U(24)$. Este é um grupo cíclico? *(1.5 ponto)*

d) Escreva uma função em Python que receba como entrada um número inteiro $n \geq 2$ e retorne uma lista com todos os subgrupos cíclicos de $U(n)$. *(1.5 ponto)*

Questão 2: Através do uso do *Método de Fermat*, encontre um fator do número de Mersenne $M(37)$ ou determine que ele é primo. *(1.5 ponto)*

Questão 3: Utilize o *Teste de Lucas Melhorado* para verificar se o número 2297 é primo ou composto. *(1.5 pontos)*

Questão 4: *(3 pontos)*

a) A mensagem abaixo foi encriptada com RSA, utilizando os parâmetros públicos listados. Quebre a criptografia e exponha o conteúdo da mensagem. *(1.5 pontos)*

- Mensagem Codificada: 4059 - 8462 - 2319
- Parâmetros públicos do RSA: $n = 12193$, $e = 7181$
- Tabela de Pré-Codificação:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

b) Criptografe o último bloco que você obteve como resposta no item anterior agora utilizando o El Gamal com parâmetros $p = 167$, $g = 5$, chave pública $c = 55$ e $k = 6$. *(1.5 ponto)*