USP/ICMSC/SMA -2ª Prova de SMA-0508-Matemática Discreta

Professor: Daniel Levcovitz

Nome: _____

N.º USP: _____ 26, 06, 2019

Testes. Nas questões abaixo escolha uma, e somente uma, das alternativas. Marque-a com caneta azul ou preta. Não será aceita nenhuma rasura nas questões testes. Todos os testes valem 1 ponto.

1. Sejam a e m inteiros primos entre si. A **ordem** de um inteiro a módulo m é o menor inteiro positivo d tal que $a^d \equiv 1 \pmod{m}$. Então a ordem de 5 módulo 13 é?

   (a) 6

   (b) 3

   (c) 2

   (d) 4

   (e) 12

2. Assinale a correta. Quais são os dois últimos dígitos de 7^{2000}?

   (a) 01

   (b) 88

   (c) 12

   (d) 33

   (e) 72

3. Sobre a segurança do RSA de chave pública $n = pq$ onde p e q são primos, podemos afirmar que:

   (a) A segurança do RSA independe dos primos p e q serem muito grandes.

   (b) O RSA é seguro pois, se os primos p e q forem muito grandes, é quase impossível fatorar n.

   (c) O RSA é seguro pois existem infinitos números primos.

   (d) A segurança do RSA depende do fato da chave n ser pública.

   (e) O RSA é seguro pois, se os primos p e q forem muito grandes, é quase impossível fatorar $(p-1)(q-1)$.

4. Sabemos que

$$2^{4060220} \equiv 3009238 \pmod{4060221}.$$

Então podemos concluir que

(a) A fatoração de 3009238 possui exatamente 2 primos distintos.

(b) A divisão de $2^{4060220}$ por 3009238 deixa resto 4060221.

(c) 4060221 não é primo.

(d) $2^{4060220}$ é múltiplo de 4060221.

(e) 4060221 é potência de um número primo.

5. O resto da divisão por 31 da potência $2^{6.556.423}$ é?

(a) 12

(b) 8

(c) 1

(d) 30

(e) 0

6. No algoritmo RSA, uma mensagem é um inteiro tal que $0 \leq m < 5.11 = 55$ e uma mensagem criptografada é

$$C(m) = m^3 \pmod{55}.$$

Qual é o valor do expoente decriptografador d? Em outras palavras, qual é um possível valor de d tal que

$$C(m)^d \equiv m \pmod{55}?$$

(a) 54

(b) 55

(c) 27

(d) 8

(e) 1

7. Sabendo que 2017 é primo, o resto da divisão de 4^{2018} por 2017 é?

(a) 16

(b) 0

(c) 4

(d) 1

(e) 2016

8. O menor inteiro positivo que deixa resto 4 na divisão por 7 e resto 5 na divisão por 11 é?

(a) 522

(b) 32

(c) 400

(d) 60

(e) 137

9. Sobre e equação $2x - 1 \equiv 7 \pmod{15}$ podemos afirmar que:

   (a) Ela possui infinitas soluções da forma $x = 4 + 15k, k \in \mathbb{Z}$.

   (b) Ela não possui solução em $\mathbb{Z}$.

   (c) Ela possui uma única solução em $\mathbb{Z}$ que é $x = 4$.

   (d) Todo inteiro $x \in \mathbb{Z}$ é solução dessa equação.

   (e) Ela é impossível.

10. Sobre o Pequeno Teorema de Fermat podemos afirmar que:

   (a) Se p é um número primo e $a \in \mathbb{Z}$ não é divisível por p então $a^{p-1} \equiv \pm 1 \pmod{p}$.

   (b) Se $n \in \mathbb{Z}$ é um número qualquer e $a \in \mathbb{Z}$ não é divisível por n então $a^{n-1} \equiv 1 \pmod{n}$.

   (c) Se $a^{p-1} \equiv 1 \pmod{p}$ então p é primo.

   (d) Se p é um número primo e $a \in \mathbb{Z}$ não é divisível por p então $a^{p-1} \equiv a \pmod{p}$.

   (e) Se p é um número primo e $a \in \mathbb{Z}$ não é divisível por p então $a^{p-1} \equiv 1 \pmod{p}$.