



# ABIN

## AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

**CARGO**

**8**

**CONCURSO PÚBLICO**

**NÍVEL SUPERIOR**

### OFICIAL TÉCNICO DE INTELIGÊNCIA ÁREA DE CRIPTOANÁLISE - ESTATÍSTICA

### Caderno de Provas Objetivas e Discursiva

#### LEIA COM ATENÇÃO AS INSTRUÇÕES ABAIXO.

- 1 Ao receber este caderno de provas, confira inicialmente se os seus dados pessoais, transcritos acima, estão corretos e coincidem com o que está registrado na sua folha de respostas e na sua folha de texto definitivo da prova discursiva. Confira também o seu nome em cada página numerada deste caderno. Em seguida, verifique se ele contém a quantidade de itens indicada em sua folha de respostas, correspondentes às provas objetivas, e a prova discursiva, acompanhada de espaço para rascunho. Caso o caderno esteja incompleto, tenha qualquer defeito ou apresente discordância quanto aos seus dados pessoais, solicite ao fiscal de sala mais próximo que tome as providências cabíveis, pois não serão aceitas reclamações posteriores nesse sentido.
- 2 Quando autorizado pelo chefe de sala, no momento da identificação, escreva, no espaço apropriado da **folha de respostas**, com a sua caligrafia usual, a seguinte frase:  
*Conhecimento e ignorância são diretamente proporcionais: quanto maior aquela, maior esta.*  
Conforme previsto em edital, o descumprimento dessa instrução implicará a anulação das suas provas e a sua eliminação do concurso.
- 3 O espaço para rascunho da prova discursiva, de uso opcional, não contará para efeito de avaliação.
- 4 Não utilize lápis, lapiseira (grafite), borracha e(ou) qualquer material de consulta que não seja fornecido pelo CESPE/UnB.
- 5 Não se comunique com outros candidatos nem se levante sem autorização do chefe de sala.
- 6 Não serão fornecidas folhas suplementares para rascunho nem para texto definitivo.
- 7 Na duração das provas, está incluído o tempo destinado à identificação — que será feita no decorrer das provas —, ao preenchimento da folha de respostas e à transcrição do texto para a folha de texto definitivo da prova discursiva.
- 8 Ao terminar as provas, chame o fiscal de sala mais próximo, devolva-lhe a sua folha de respostas e a sua folha de texto definitivo e deixe o local de provas.
- 9 A desobediência a qualquer uma das determinações constantes em edital, no presente caderno, na folha de respostas ou na folha de texto definitivo poderá implicar a anulação das suas provas.

#### OBSERVAÇÕES

- Não serão conhecidos recursos em desacordo com o estabelecido em edital.
- Informações adicionais: telefone 0(XX) 61 3448-0100; Internet – [www.cespe.unb.br](http://www.cespe.unb.br).
- É permitida a reprodução deste material apenas para fins didáticos, desde que citada a fonte.

- De acordo com o comando a que cada um dos itens a seguir se refira, marque, na **folha de respostas**, para cada item: o campo designado com o código **C**, caso julgue o item **CERTO**; ou o campo designado com o código **E**, caso julgue o item **ERRADO**. A ausência de marcação ou a marcação de ambos os campos não serão apenadas, ou seja, não receberão pontuação negativa. Para as devidas marcações, use a **folha de respostas**, único documento válido para a correção das suas provas objetivas.
- Nos itens que avaliam conhecimentos de informática, a menos que seja explicitamente informado o contrário, considere que todos os programas mencionados estão em configuração padrão, em português, que o *mouse* está configurado para pessoas destros, que expressões como **clicar**, **clique simples** e **clique duplo** referem-se a cliques com o botão esquerdo do *mouse* e que **teclar** corresponde à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Considere também que não há restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados.

## CONHECIMENTOS GERAIS

### Texto para os itens de 1 a 11

1 Nas últimas décadas, o aumento dos índices de  
 4 criminalidade e a atuação de organizações criminosas  
 7 transnacionais colocaram a segurança pública entre as  
 10 principais preocupações da sociedade e do Estado brasileiros.  
 13 A delinquência e a violência criminal afetam, em maior ou  
 16 menor grau, toda a população, provocando apreensão e medo  
 19 na sociedade, e despertando o sentimento de descrença em  
 22 relação às instituições estatais responsáveis pela manutenção da  
 25 paz social.

26 No projeto Segurança Pública para o Brasil, da  
 29 Secretaria Nacional de Segurança Pública, aponta-se como  
 32 principal causa do aumento da criminalidade o tráfico de  
 35 drogas e de armas. A articulação entre esses dois ilícitos  
 38 potencializa e diversifica as atividades criminosas. Homicídios  
 41 dolosos, roubos, furtos, sequestros e latrocínios estão,  
 44 frequentemente, associados ao consumo e venda de drogas e à  
 47 utilização de armas ilegais.

48 Mundialmente, o tripé integrado por narcotraficantes,  
 51 terroristas e contrabandistas de armas atua em conjunto ou de  
 54 forma complementar, constituindo uma grave ameaça à  
 57 sociedade e aos Estados nacionais. A globalização favoreceu  
 60 a expansão geográfica dos crimes transnacionais, cujos agentes  
 63 utilizam as facilidades comerciais, as comunicações e os  
 66 múltiplos meios de transportes para encobrir suas atividades  
 69 ilícitas.

70 Em razão da complexidade, da amplitude e do poderio  
 73 das redes criminosas transnacionais, a solução para a  
 76 criminalidade depende de decisões político-econômico-sociais  
 79 e, concomitantemente, de ações preventivas e repressivas de  
 82 órgãos estatais. Nesse contexto, as operações de inteligência  
 85 são instrumentos legais de que dispõe o Estado na busca pela  
 88 manutenção e proteção de dados sigilosos.

89 A Agência Brasileira de Inteligência (ABIN), órgão  
 92 central do Sistema Brasileiro de Inteligência (SISBIN), deve  
 95 assumir a missão de centralizar, processar e distribuir dados e  
 98 informações estratégicas para municiar os órgãos policiais  
 101 (federais, estaduais e municipais) nas ações de combate ao  
 104 crime organizado. Além disso, a ABIN é responsável por  
 107 manter contato com os serviços de inteligência parceiros, para  
 110 favorecer a troca de informações e a cooperação multilateral.

Cristina Célia Fonseca Rodrigues. A atividade operacional em benefício da segurança pública: o combate ao crime organizado. In: Revista Brasileira de Inteligência. Brasília: ABIN, n.º 5, out./2009. Internet: <www.abin.gov.br> (com adaptações).

Com relação às ideias do texto, julgue os itens seguintes.

- 1 O argumento de que a criminalidade é intensificada pela associação do narcotráfico com o contrabando de armas reforça a ideia central do texto, que pode ser expressa nos seguintes termos: os serviços de inteligência são imprescindíveis para a redução da criminalidade no mundo.
- 2 De acordo com o texto, o processo de globalização é o principal responsável pelo aumento dos índices de criminalidade no Brasil.
- 3 Infere-se do texto que as autoridades do Estado devem valer-se dos serviços de inteligência para combater o crime organizado.
- 4 Depreende-se da leitura do texto que uma das razões para o descrédito das instituições responsáveis pela segurança pública é a corrupção existente entre seus membros.
- 5 Das informações do texto conclui-se que o intercâmbio de dados e informações entre agências de inteligência coíbe a expansão de redes criminosas.
- 6 Considerando-se que as operações de inteligência são instrumentos legais disponíveis ao Estado, é correto inferir que os serviços de inteligência prescindem das formalidades legais para a obtenção de dados sigilosos.

Com referência às estruturas linguísticas empregadas no texto, julgue os itens subsequentes.

- 7 A supressão das vírgulas que isolam a expressão “da Secretaria Nacional de Segurança Pública” (ℓ.10-11) alteraria o sentido do texto, visto que estaria subentendida a existência de, pelo menos, mais um projeto denominado Segurança Pública para o Brasil.
- 8 Na linha 31, a preposição “de” empregada antes de “que” é exigência sintática da forma verbal “dispõe”; portanto, sua retirada implicaria prejuízo à correção gramatical do período.
- 9 A substituição do termo “estratégicas” (ℓ.36) por **estratégicos** não causaria prejuízo à correção gramatical nem ao sentido do texto.
- 10 A substituição da expressão “ao crime organizado” (ℓ.37-38) por **à criminalidade** alteraria o sentido original do texto, mas não prejudicaria a correção gramatical do período.
- 11 Estaria gramaticalmente correto o emprego da preposição **a** antes de “toda a população” (ℓ.6) — **a toda a população** — visto que a forma verbal “afetam” (ℓ.5) apresenta dupla regência.

Os itens a seguir são excertos adaptados do texto **A atividade operacional em benefício da segurança pública: o combate ao crime organizado** (*op. cit.*). Julgue-os no que se refere à correção gramatical e à coerência das ideias.

- 12 A globalização do crime e as perspectivas de crescimento das organizações criminosas transnacionais com ampliação de redes de atuação e constantes inovações no modo de ação exige dos Estados nacionais atividades coordenadas a nível de segurança pública.
- 13 Para combater, eficientemente, as diversas modalidades de crimes transnacionais é preciso penetrar na hierarquia compartimentalizada das organizações criminosas para conhecer seus objetivos e ligações e antecipar suas ações.
- 14 Os crimes transnacionais proliferam à velocidade altíssima, por conseguinte, beneficiam-se do avanço das telecomunicações, razão porque a inteligência torna-se essencial para o combate dos mesmos.
- 15 Os dados e as informações reunidas pelas operações de inteligência possibilitam a identificação e a compreensão das características, da estrutura, das formas de financiamento e do modo de operação das organizações criminosas e de seus componentes.

---

Considere que, em um órgão de inteligência, o responsável por determinado setor disponha de 20 agentes, sendo 5 especialistas em técnicas de entrevista, 8 especialistas em reconhecimento operacional e 7 especialistas em técnicas de levantamento de informações, todos com bom desempenho na tarefa de acompanhamento de investigado. A partir dessas informações, julgue os itens a seguir.

- 16 Considere que uma das técnicas de acompanhamento de investigado que se desloque por uma rua retilínea consista em manter um agente no mesmo lado da via que o investigado, alguns metros atrás deste, e dois outros agentes do lado oposto da rua, um caminhando exatamente ao lado do investigado e outro, alguns metros atrás. Nessa situação, há 10 maneiras distintas de 3 agentes previamente escolhidos se organizarem durante uma missão de acompanhamento em que seja utilizada essa técnica.
- 17 Há mais de 270 maneiras distintas de o responsável pelo setor organizar uma equipe composta por 1 especialista em entrevista, 1 em reconhecimento operacional e 1 em levantamento de informações, para determinada missão.
- 18 Se, para cumprir determinada missão, for necessário fazer, simultaneamente, reconhecimento operacional em 3 locais diferentes, então o responsável pelo setor terá 340 maneiras distintas de compor uma equipe da qual façam parte 3 agentes especialistas para essa missão, sendo um especialista para cada local.

Um entrevistador obteve de um suspeito a seguinte declaração: “Ora, se eu fosse um espião, então eu não amaria o meu país, pois eu amo o meu país, ou sou um traidor da pátria, já que não é possível acontecer as duas coisas ao mesmo tempo. Agora, se eu não fosse um traidor da pátria, então eu amaria o meu país. Logo, eu não sou um espião e amo o meu país.”

Considerando a lógica sentencial apresentada, julgue os itens subsequentes.

- 19 O argumento do suspeito é um argumento válido.
- 20 A negação da conclusão do argumento utilizado pelo suspeito é equivalente à seguinte proposição: “eu sou um espião ou não amo o meu país”.

Acerca do uso de ferramentas, técnicas e aplicativos para a Internet e *intranet*, julgue os itens que se seguem.

- 21 A utilização dos padrões de correio eletrônico implica a geração automática, pelo IMAP (*Internet message access protocol*), de uma assinatura digital, que pode ser verificada pelo destinatário.
- 22 A troca de mensagens eletrônicas entre cidades geograficamente distantes não pode ser realizada por meio de uma *intranet*, em razão das características dos protocolos de *email* usados em uma rede corporativa.

Com relação ao ambiente Microsoft Office, julgue os próximos itens.

- 23 Uma planilha criada no Excel 2007 e armazenada em arquivo no formato *xlsx* pode ser exportada para o padrão XML, por meio do próprio Excel 2007.
- 24 Um documento criado no Word 2003 pode ser aberto no Word 2007 e salvo no formato *docx*.

Julgue o item abaixo, a respeito de mecanismos de segurança da informação, considerando que uma mensagem tenha sido criptografada com a chave pública de determinado destino e enviada por meio de um canal de comunicação.

- 25 A mensagem criptografada com a chave pública do destinatário garante que somente quem gerou a informação criptografada e o destinatário sejam capazes de abri-la.

Com base na Lei n.º 9.883/1999, que instituiu o SISBIN e criou a ABIN, julgue os seguintes itens.

- 26 Os atos administrativos, no âmbito da ABIN, que viabilizem aquisições de bens e serviços cuja publicidade possa comprometer o êxito das atividades sigilosas da agência devem ser publicados em extrato, cabendo ao gestor utilizar, nesses casos, recursos orçamentários sigilosos.
- 27 O controle e a fiscalização externos da atividade de inteligência são exercidos pela Comissão Mista de Controle de Órgãos de Inteligência do Congresso Nacional, criada junto com a ABIN. Integram-na os presidentes das Comissões de Relações Exteriores e Defesa Nacional da Câmara dos Deputados e do Senado Federal, os líderes da maioria e minoria na Câmara dos Deputados e no Senado Federal e o presidente do Tribunal de Contas da União.

De acordo com o que dispõe o Decreto n.º 4.376/2002 sobre a organização e funcionamento do SISBIN, julgue os próximos itens.

- 28 Exige-se, nas reuniões do conselho consultivo do SISBIN presença de, no mínimo, dois terços de seus membros.
- 29 As unidades da Federação podem compor o SISBIN, mediante ajustes específicos e convênios e aprovação necessária do conselho consultivo instituído pelo referido decreto.

Considerando os direitos, as obrigações e as competências dos ocupantes de cargos e funções da ABIN, julgue os itens que se seguem com base no disposto na Lei n.º 11.776/2008 e no Decreto n.º 6.408/2008.

- 30 A cessão dos titulares de cargos integrantes do quadro de pessoal da ABIN só é permitida para os casos previstos em legislação específica ou investidura em cargo de natureza especial ou do grupo de direção e assessoramento superiores (DAS), nos níveis 4, 5 e 6, ou equivalentes.
- 31 A propriedade intelectual criada por qualquer agente público em decorrência do exercício de suas atribuições ou na condição de representante da ABIN pertence exclusivamente à União, determinação que não abrange a produção intelectual dos alunos de cursos ministrados pelo órgão, nem patentes requeridas por ex-servidor da ABIN depois de decorrido um ano após a extinção do seu vínculo empregatício.

Julgue os próximos itens com base no que estabelece o Código Penal sobre falsidade documental e crimes praticados por funcionário público.

- 32 O funcionário que inserir ou facilitar, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da administração pública com o fim de obter vantagem indevida para si ou para outrem, ou para causar dano está sujeito a pena de reclusão de dois a doze anos, e multa, devendo, ainda, as penas ser aumentadas de um terço até a metade se a modificação ou alteração resultar em dano para a administração pública ou para o administrado.
- 33 A omissão, em documento público, de declaração que dele deveria constar, ou a inserção de declaração falsa ou diversa da que deveria ter sido escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato jurídico relevante, sujeita o funcionário público a pena de reclusão de um a cinco anos e multa, se o documento for público; e de um a três anos e multa, se o documento for particular. A pena será aumentada em um sexto se a falsificação ou alteração for de assentamento de registro civil.

Julgue os próximos itens, relativos à salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da administração pública federal.

- 34 A preparação, impressão ou, se for o caso, reprodução de documento sigiloso efetuada em tipografias, impressoras, oficinas gráficas ou similares devem ser acompanhadas por pessoa oficialmente designada para tanto, sendo ela responsável pela garantia do sigilo durante a confecção do documento e pela eliminação de notas manuscritas, tipos, clichês, carbonos, provas ou qualquer outro recurso que possa dar origem a cópia não autorizada do todo ou parte.
- 35 Os equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo secreto, confidencial e reservado só podem integrar redes de computadores que possuam sistemas de criptografia e segurança adequados à proteção dos documentos e que sejam física e logicamente isoladas de qualquer outra.
- 36 Os titulares de órgãos ou entidades públicos encarregados da preparação de planos, pesquisas e trabalhos de aperfeiçoamento ou de novo projeto, prova, produção, aquisição, armazenagem ou emprego de material sigiloso são os responsáveis pela expedição das instruções adicionais que se tornarem necessárias à salvaguarda dos assuntos a eles relacionados.
- 37 Os órgãos e entidades públicos e as instituições de caráter público, para dar conhecimento de minuta de contrato cujo objeto seja sigiloso ou cuja execução implique a divulgação de desenhos, plantas, materiais, dados ou informações de natureza sigilosa devem exigir dos interessados na contratação a assinatura de termo de compromisso de manutenção do sigilo.

Acerca da Política de Segurança da Informação (PSI) nos órgãos e entidades da administração pública federal, instituída pelo Decreto n.º 3.505/2000, julgue os seguintes itens.

- 38 Cabe à Secretaria de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação e pelo Departamento de Pesquisa e Desenvolvimento Tecnológico da ABIN, estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos criptográficos, de modo a assegurar-lhes confidencialidade, autenticidade e integridade, assim como a garantir a interoperabilidade entre os sistemas de segurança da informação.
- 39 Os membros do Comitê Gestor da Segurança da Informação só podem participar de processos, no âmbito da segurança da informação, de iniciativa do setor privado, caso essa participação seja julgada imprescindível para atender aos interesses da defesa nacional, a critério do Comitê Gestor e após aprovação do Gabinete de Segurança Institucional da Presidência da República.
- 40 Entre os objetivos da PSI, insere-se o estímulo à participação competitiva do setor produtivo no mercado de bens e de serviços relacionados com a segurança da informação, incluindo-se a fabricação de produtos que incorporem recursos criptográficos.

Julgue os itens seguintes, acerca da segurança pública e das Forças Armadas.

- 41 As corporações consideradas forças auxiliares e reserva do Exército subordinam-se aos governadores dos estados, do Distrito Federal e dos territórios.
- 42 Segundo entendimento do Supremo Tribunal Federal, os aspectos relativos à legalidade da imposição de punição constritiva da liberdade, em procedimento administrativo castrense, podem ser discutidos por meio de *habeas corpus*.
- 43 É permitido a um estado da Federação criar instituto geral de perícias estadual e inseri-lo no rol constitucional dos órgãos encarregados do exercício da segurança pública.

Com referência a aspectos constitucionais, julgue os itens que se seguem.

- 44 Embora seja da competência da União legislar sobre defesa territorial, na hipótese de ocorrência de omissão legislativa acerca desse tema, aos estados-membros é concedida autorização constitucional para o exercício da competência legislativa suplementar.
- 45 A soberania popular é exercida, em regra, por meio da democracia representativa. A Constituição Federal brasileira consagra, também, a democracia participativa ao prever instrumentos de participação intensa e efetiva do cidadão nas decisões governamentais.

Julgue os itens subsequentes, a respeito dos poderes e atos administrativos.

- 46 A revogação de um ato revogador não restaura, automaticamente, a validade do primeiro ato revogado.
- 47 Considere a seguinte situação hipotética.  
Um município estabeleceu que somente seriam concedidos alvarás de funcionamento a restaurantes que tivessem instalado exaustor de fumaça acima de cada fogão industrial. Na vigência dessa determinação, um fiscal do município atestou, falsamente, que o restaurante X possuía o referido equipamento, tendo-lhe sido concedido o alvará. Dias após a fiscalização, a administração verificou que não havia no referido estabelecimento o exaustor de fumaça.  
Nessa situação hipotética, considera-se nulo o alvará, dada a inexistência de motivo do ato administrativo.
- 48 A licença é um ato administrativo que revela o caráter preventivo da atuação da administração no exercício do poder de polícia.

No que se refere ao regime jurídico dos servidores públicos civis da administração federal, julgue os itens a seguir.

- 49 O servidor público removido de ofício, no interesse da administração, pode alegar a garantia da inamovibilidade para permanecer no local onde exerce suas funções.
- 50 Afasta-se a responsabilidade penal do servidor público que pratique fato previsto, na legislação, como contravenção penal, dada a baixa lesividade da conduta, subsistindo a responsabilidade civil e administrativa.

## CONHECIMENTOS ESPECÍFICOS

RASCUNHO

Considerando que a distribuição gama, definida pelos parâmetros  $n$  e  $\lambda$ , em que  $n$  é um número inteiro e  $\lambda$ , um número real maior que zero, é caracterizada como a soma de  $n$  variáveis aleatórias independentes com distribuição exponencial com média  $\frac{1}{\lambda}$ , julgue os itens que se seguem.

- 51 Considere que  $Y_1, \dots, Y_n$  seja uma amostra aleatória simples retirada de uma distribuição exponencial com média  $\frac{1}{\lambda}$  e que  $Y = \sum_{i=1}^n Y_i$ . Nessa situação, é correto afirmar que  $\frac{Y_1}{Y}, \dots, \frac{Y_n}{Y}$  são variáveis aleatórias independentes e identicamente distribuídas e que o espaço amostral de  $\frac{Y_i}{Y}$  ( $i = 1, \dots, n$ ) é o intervalo  $[0, \infty[$ .
- 52 Considere que uma amostra aleatória simples retirada dessa distribuição gama tenha produzido uma média aritmética igual a 20 e uma variância amostral igual a 50. Nessa situação, as estimativas dos parâmetros  $n$  e  $\lambda$ , pelo método de momentos, são respectivamente iguais a 8 e 0,4.

Considerando a função  $f(x) = \frac{1}{c} \left( x + \frac{1}{2} \right)^2$ , em que  $0 \leq x \leq 1$  e  $c$ , uma constante de normalização, julgue os itens que se seguem.

- 53 Se  $f(x) > 1$  para algum  $x \in [0, 1]$ , então a função  $f(x)$  não é uma função de densidade.
- 54 A função  $f(x)$  é uma função de densidade de uma variável aleatória se  $c = \frac{13}{12}$ .

Sabendo que  $X$  é variável aleatória discreta que pode assumir valores inteiros não negativos, julgue os próximos itens.

- 55 A média de  $X$  é não negativa.
- 56 Considere que  $P(X=0) = 1 - \phi(\tau)$  e  $P(X=k) = \phi(\tau)P(X=k-1)$ , em que  $\tau$  é um parâmetro,  $0 \leq \phi(\tau) \leq 1$  e  $k \geq 1$ . Nessa situação, é correto afirmar que a média de  $X$  é maior que  $\frac{1}{2}$  se  $\phi(\tau) < \frac{1}{3}$ .
- 57 A esperança de  $X$  é igual a  $\sum_{k=1}^{+\infty} P(X \geq k)$ .

Sabendo que  $X$  é uma variável aleatória discreta,  $0 < p < 1$  e  $k$ , número natural, julgue o item abaixo.

- 58  $P(X \leq k) = (1 - p)^k$  é uma função de probabilidade acumulada.

A respeito da distribuição binomial  $X$  com parâmetros  $n$  e  $p$ , em que  $n \geq 1$  e  $0 < p < 1$ , julgue os itens subsequentes.

59 Se  $n$  for suficientemente grande, então é correto afirmar que

$$P(X = k) \cong \Phi\left(\frac{k + 0,5 - np}{\sqrt{np(1-p)}}\right) - \Phi\left(\frac{k - 0,5 - np}{\sqrt{np(1-p)}}\right),$$

em que  $\Phi$  é a função de distribuição acumulada da normal padrão.

60 Considerando-se que  $Y$  siga uma distribuição binomial com parâmetros  $m$  e  $p$  e que  $X$  e  $Y$  sejam variáveis aleatórias independentes, é correto afirmar que a soma  $X + Y$  segue uma distribuição binomial com parâmetros  $(n + m)$  e  $p$ .

61 No caso assintótico em que  $\lim_{\substack{n \rightarrow \infty \\ p \rightarrow 0}} np = \lambda > 0$ , então  $P(X > 0) \cong 1 - e^{-\lambda}$ .

62 Considere a seguinte situação hipotética.

De uma urna que contém 15 bolas brancas e 1 bola vermelha serão retiradas aleatoriamente 12 bolas. Em cada retirada, será observada a cor da bola selecionada. Se branca, a bola não será devolvida à urna; se vermelha, a bola será devolvida à urna. Ao final do processo, será registrado o número  $X$  de vezes que a bola vermelha foi observada nessas doze retiradas.

Em face dessa situação, é correto afirmar que  $X$  é uma variável aleatória com distribuição binomial com  $n = 12$ .

A função de densidade da distribuição normal padrão  $Z$  é dada pela

função  $f(z) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{z^2}{2}\right)$ , em que  $z$  é um número real.

Considerando a transformação  $Y = \exp(Z)$ , julgue o item a seguir.

63 A função de densidade da variável aleatória  $Y$  é

$$f(y) = \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{[\exp(y)]^2}{2}\right\}, \text{ em que } y \geq 0.$$

opinião1	opinião 2		total
	satisfeito	insatisfeito	
satisfeito	$x_{11}$	$x_{12}$	$x_{1\cdot} = x_{11} + x_{12}$
insatisfeito	$x_{21}$	$x_{22}$	$x_{2\cdot} = x_{21} + x_{22}$
total	$x_{\cdot 1} = x_{11} + x_{21}$	$x_{\cdot 2} = x_{12} + x_{22}$	$n$

Considerando que a tabela de contingência acima mostra os resultados de um levantamento estatístico, julgue os itens que se seguem.

64 A estatística do teste qui-quadrado para independência é

$$E_{ij} = \frac{x_{i\cdot} + x_{\cdot j}}{n}.$$

65 A hipótese nula do teste de homogeneidade de McNemar é  $H_0$ :

$$x_{ij} = x_{i\cdot} x_{\cdot j}, \text{ em que } i, j = 1, 2.$$

Com relação aos testes qui-quadrado, julgue o item a seguir.

66 O teste qui-quadrado permite verificar a aderência de um conjunto de dados com relação a determinada distribuição de probabilidade.

Julgue o próximo item, acerca de análise de variância ANOVA.

67 A ANOVA consiste em teste de hipótese para avaliar se os diferentes tratamentos de um experimento produzem as mesmas variâncias com relação a determinada variável resposta  $Y$ .

Julgue os itens subsequentes, relativos a planejamento fatorial.

68 Em um planejamento fatorial fracionário, o estimador da média global é viciado.

69 Considere a situação em que haja dois tratamentos A e B.

Nessa situação, a matriz de delineamento

$$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

refere-se a um planejamento fatorial fracionário.

70 Considerando-se três tratamentos, A, B e C, em um planejamento fatorial fracionário  $2^{3-1}$ , conclui-se que o tratamento A está confundido com a interação entre os tratamentos B e C.

Acerca de planejamento do tipo quadrado latino, julgue o próximo item.

71 A variável resposta é avaliada em todas as combinações possíveis de tratamentos.

Considerando que as variáveis  $X$  e  $Y$  estejam relacionadas de forma não linear, julgue o item abaixo.

72 O valor absoluto da correlação de Pearson entre  $X$  e  $Y$  é maior que o valor absoluto da correlação de Spearman entre essas variáveis.

Considerando que os conceitos de inferência estatística são fundamentais para a análise estatística, julgue os itens a seguir.

73 Considere uma distribuição cuja função de densidade tenha a forma  $f(x) = \exp\{S(\theta)T(x) + h(x) + c(\theta)\}$ , em que  $\theta$  é o parâmetro desconhecido da distribuição,  $S$  e  $c$  são funções que dependem somente de  $\theta$ , e  $T$  e  $h$  são funções que dependem somente de  $x$ . Nessa situação, pela regra da fatoração,  $S(\theta)$  é estatística suficiente para o parâmetro  $\theta$ .

74 Suponha que  $T(X)$  seja uma estatística suficiente para o parâmetro  $\theta$  de uma distribuição  $X$ . Nessa situação, para estimar o parâmetro  $\theta$ , basta obter uma realização da estatística  $T(X)$ .

Com relação a métodos não paramétricos, julgue os itens a seguir.

- 75 Considere que, para avaliar a aleatoriedade na ocorrência de certo evento, um pesquisador registre apenas o número de ocorrências desse evento em  $N$  tentativas, a contagem de casos em que esses eventos ocorrem sequencialmente e a contagem de casos em que esses eventos não ocorrem. Com base nessa situação, é correto afirmar que o pesquisador não dispõe de dados necessários para testar a aleatoriedade desse evento.
- 76 O teste de Wilcoxon é o equivalente não paramétrico do teste  $t$ -Student para comparação de duas médias, e o teste de Kruskal-Wallis é o equivalente não paramétrico da análise de variâncias para um fator.
- 77 Hipóteses acerca da mediana de certa população podem ser avaliadas pelo teste dos sinais.

Considerando a matriz de transição  $M = \begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{3}{4} & \frac{1}{4} \end{bmatrix}$ , julgue os próximos

itens acerca de cadeias de Markov.

- 78 O vetor de distribuição do processo no limite estacionário é

$$\pi = \begin{bmatrix} \frac{9}{17} \\ \frac{8}{17} \end{bmatrix}.$$

- 79 A matriz de probabilidades de transição no segundo passo é

$$M^{(2)} = \begin{bmatrix} \frac{11}{16} & \frac{7}{16} \\ \frac{18}{7} & \frac{9}{16} \end{bmatrix}.$$

Considerando uma cadeia de Markov, com matriz de transição

$$M = \begin{bmatrix} p & 1-p \\ 1-q & q \end{bmatrix}, \text{ em que } 0 \leq p, q \leq 1, \text{ julgue os seguintes itens.}$$

- 80 Todo processo de Markov com dois estados é duplamente estocástico.
- 81 O processo não possui limite estacionário se  $p=1$  e  $q=1$ .

Considerando que o passeio aleatório simples seja dado por  $\{S_n\}_{n \geq 1}$ ,

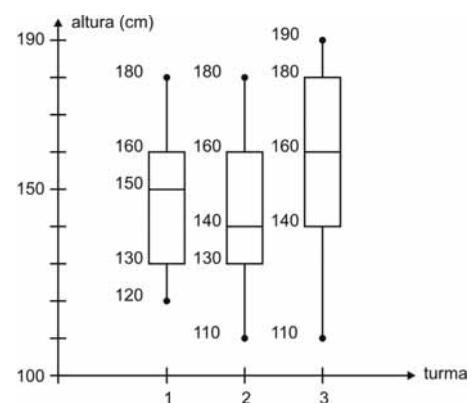
em que  $S_n = \sum_{i=1}^n X_i$ ,  $P(X_i = 1) = p$ ,  $P(X_i = -1) = 1 - p$ , e  $0 < p < 1$ ,

julgue os seguintes itens acerca desse processo estocástico.

- 82 O passeio aleatório simples não é uma cadeia de Markov.
- 83 No passo 1 ( $n=1$ ), o passeio aleatório pode assumir valor  $-1$  ou  $1$ . Logo, nos passos pares  $2n$ , esse processo assume valor par (inclusive o valor zero) com probabilidade 1; nos passos ímpares  $2n+1$ , esse mesmo processo assume valor ímpar com probabilidade 1.

Sabendo que o número de veículos que chegam, a cada minuto, a determinado local de uma avenida segue um processo de Poisson homogêneo, julgue os itens a seguir.

- 84 Considere que uma contagem de tempo seja iniciada no instante em que um veículo A passe nesse local, e que a partir desse, a contagem se encerre no momento da passagem do décimo veículo. Nessa situação, a distribuição desse tempo entre o primeiro e o décimo veículo segue uma distribuição gama.
- 85 O intervalo de tempo entre um veículo e o veículo consecutivo segue uma distribuição exponencial.



A figura acima apresenta esquematicamente as distribuições das alturas (em cm) dos estudantes das três turmas de uma escola. As linhas verticais de cada *box-plot* se estendem até os valores extremos da distribuição. Com base nessas informações, julgue os itens consecutivos.

- 86 A turma 3 tem a maior amplitude de alturas.
- 87 As distribuições das alturas referentes às turmas 2 e 3 são simétricas.
- 88 Entre os estudantes da turma 1, 75% possuem alturas iguais ou superiores a 160 cm, enquanto metade dos estudantes da turma 3 tem altura igual ou inferior a 160 cm.

2	1 3 2 6
3	4 3 5 8 7
4	6 2 1 9 6
5	4 2 0 5

Considerando que o diagrama de ramos-e-folhas acima mostra a distribuição das idades (em anos) dos servidores de determinada repartição pública, julgue os próximos itens.

- 89 O primeiro quartil e o terceiro quartil são, respectivamente, 34 e 46 anos de idade.
- 90 A mediana das idades dos servidores é igual a 39,5 anos.



RASCUNHO

estação	altitude (em km)	temperatura (em °C)
1	1	20
2	2	10
3	4	5
4	5	5

Com base nas informações da tabela acima, que mostra as temperaturas registradas em determinado horário e dia, em quatro estações meteorológicas, e as altitudes em que cada uma dessas estações se encontra, julgue o seguinte item.

- 91 Considerando que a relação entre graus Fahrenheit e graus Celsius é dada por  $F = 1,8 C + 32$ , é correto afirmar que a correlação linear de Pearson entre as altitudes e as temperaturas é maior quando calculada com as temperaturas em graus Fahrenheit que quando calculada em graus Celsius.

empregados	gênero		total
	masculino	feminino	
fumantes	40	10	50
não fumantes	80	70	150
total	120	80	200

O chefe de uma empresa pediu um estudo estatístico para avaliar a associação entre o hábito de fumar e o gênero dos seus empregados. O resultado desse estudo está resumido na tabela de contingência acima. Com base nessas informações, julgue os itens a seguir.

- 92 O coeficiente de contingência modificado foi igual a  $\sqrt{\frac{2}{19}}$ .
- 93 O coeficiente de contingência modificado  $C^*$  é uma medida que permite avaliar tendências em uma tabela de contingência  $2 \times 2$ . Se  $C^*$  fosse superior a 0,9, seria correto inferir, com base unicamente nesse valor, que a porcentagem de fumantes entre as pessoas do gênero masculino seria maior do que a porcentagem de fumantes entre as pessoas do gênero feminino.
- 94 Sob a hipótese de independência entre o hábito de fumar e o gênero, o número esperado de fumantes do gênero masculino seria igual a 35.

idade (anos)	vezes por semana			total
	até 2	de 2 a 4	mais de 4	
20 a 40	40	50	40	130
40 a 60	40	20	10	70
total	80	70	50	200

O dono de uma academia coletou dados para estudar a associação entre a faixa etária dos seus alunos e a frequência de atividades desses alunos na sua academia. Os dados coletados estão resumidos na tabela de contingência acima. Com base nessas informações, julgue os itens subsequentes, acerca do coeficiente  $\gamma$  de Goodman e Kruskal.

- 95 O valor do coeficiente  $\gamma$  foi menor que  $-0,5$ .
- 96 Os números de pares concordantes e discordantes foram iguais a 1.700 e 4.400, respectivamente.

## RASCUNHO

No caso da amostragem em populações finitas deve-se multiplicar o erro padrão da média amostral pelo fator de correção  $\sqrt{\frac{N-n}{N-1}}$ , em que  $N$  e  $n$  representam o tamanho da população e da amostra, respectivamente. Na prática, esse fator é aplicado quando a fração amostral  $\frac{n}{N}$  for superior a 0,05. Com respeito a esse assunto, julgue os itens a seguir.

- 97 Para uma população de tamanho superior a 100 e uma fração amostral superior a 20%, o fator de correção será inferior a 0,9.
- 98 Se a fração amostral for inferior a 5%, então o fator de correção será superior a 0,97.

Considere que um estudo tenha sido realizado para estimar a média das idades dos empregados de determinado segmento de empresas, e que, na ocasião em que o estudo foi realizado, o tamanho da população de funcionários era  $N = 5.000$  funcionários. Essa população foi estratificada em três grupos de tamanhos  $N_1 = 1.000$ ,  $N_2 = 1.500$  e  $N_3 = 2.500$ . Da população de funcionários, foi retirada uma amostra aleatória estratificada de tamanho  $n = 100$  com alocação proporcional ao tamanho dos estratos.

estrato	média das idades (em anos)	desvio padrão das idades (em anos)
1	30	5
2	40	5
3	50	10

Considerando que o quadro acima mostra os resultados do estudo hipotético em apreço, julgue os itens subsecutivos.

- 99 O erro padrão do estimador da idade média é menor que  $\sqrt{30}$ .
- 100 A amostra foi composta de 30 empregados do estrato 1, 20 empregados do estrato 2, e 50 empregados do estrato 3.
- 101 A estimativa da média populacional das idades foi igual a 44 anos.

Determinada fábrica produz certo tipo de peça. As peças produzidas são remetidas aos consumidores em lotes de tamanho  $N$ , mas é possível que esses lotes contenham peças defeituosas. Um cliente, para avaliar a qualidade das peças de certo lote, efetua uma amostragem aleatória simples sem reposição de tamanho  $n = \frac{N}{10}$ .

Com base nessas informações, e considerando que o lote examinado pelo cliente possui exatamente 4% de peças defeituosas, julgue o item subsequente.

- 102 Se  $N = 100$ , a probabilidade de não haver peças defeituosas na amostra será inferior a 0,3.

Suponha que a variável aleatória contínua  $X$  tenha a função densidade de probabilidade

$$f(x) = \begin{cases} ax^{a-1} & \text{se } 0 \leq x \leq 1 \\ 0 & \text{caso contrário} \end{cases}$$

em que  $a > 0$ . Considerando que  $\{X_1, \dots, X_n\}$  representa uma amostra aleatória simples dessa população  $X$ , julgue os itens que se seguem, referentes à estimação pontual do parâmetro  $a$ .

103 A equação  $\hat{a} = \frac{\bar{X}}{1 - \bar{X}}$ , em que  $\bar{X}$  denota a média da amostra, é o estimador de momentos, usando o primeiro momento.

104 O estimador de máxima verossimilhança é  $\hat{a} = \frac{n}{\sum_{i=1}^n \ln X_i}$ .

Considerando que  $\hat{\theta}_1$  e  $\hat{\theta}_2$  sejam estimadores de um mesmo parâmetro  $\theta \neq 0$ , tais que  $E(\hat{\theta}_1) = \theta$ ,  $E(\hat{\theta}_2) = \frac{2}{3}\theta$ ,  $\text{Var}(\hat{\theta}_1) = 10$ ,  $\text{Var}(\hat{\theta}_2) = 5$ , e que o erro quadrático médio de um estimador seja definido como  $\text{EQM}(\hat{\theta}) = E(\hat{\theta} - \theta)^2$ , julgue os itens a seguir.

105 Considerando que  $\theta^2 < 45$ , é correto afirmar que o estimador  $\hat{\theta}_2$  é mais eficiente que  $\hat{\theta}_1$ .

106 Os estimadores  $\hat{\theta}_1$  e  $\hat{\theta}_2$  não são viciados.

O tempo de duração de determinado aparelho eletrônico segue uma distribuição normal com média desconhecida  $\mu$  e desvio padrão  $\sigma = 400$  horas. Um estudo feito com uma amostra de  $n = 1.600$  aparelhos produziu um tempo médio de duração igual a 5.000 horas. Com base nessas informações, e considerando que  $Z_{0,025} = 1,96$ , em que  $Z_\alpha$  é definido por  $\Phi(Z_\alpha) = 1 - \alpha$  e  $\Phi$  representa a função de distribuição acumulada da distribuição normal padrão, julgue os próximos itens.

107 Considerando que  $\sigma$  e  $n$  sejam valores constantes, se o nível de confiança aumentar, o comprimento do intervalo de confiança diminuirá.

108 Considere um intervalo assimétrico de 95% de confiança para a média  $\mu$  na forma  $[\bar{x} - \varepsilon_1, \bar{x} + \varepsilon_2]$ , em que  $\varepsilon_1 \neq \varepsilon_2$ ,  $\varepsilon_1 > 0$ ,  $\varepsilon_2 > 0$ . Nesse caso, o comprimento  $\varepsilon_1 + \varepsilon_2$  do intervalo assimétrico sempre será maior que o do intervalo de confiança simétrico de 95%.

109 Se o desvio padrão  $\sigma$  fosse desconhecido, o intervalo de confiança simétrico de 95% de confiança para a média  $\mu$  poderia ser dado por  $\bar{x} \pm Z_{0,025} \times \frac{s}{\sqrt{1.600}}$ , em que  $s$  representa o desvio padrão amostral.

110 A estimativa pontual para o tempo médio  $\mu$  foi superior a 500 horas.

111 Um intervalo de confiança de 95% para essa estimativa é dado por  $[380,4; 419,6]$ .

112 Se o tamanho da amostra for de 6.400 aparelhos (com  $\sigma = 400$  inalterado), o erro máximo provável de 95% da estimativa seria menor que 10 horas.

As distribuições das alturas de pessoas adultas de duas civilizações A e B possuem os seguintes parâmetros.

civilização	altura média(em $\mu$ cm)	desvio padrão (em cm)
A	176	10
B	180	20

Considere que os habitantes de uma ilha possam ser descendentes das civilizações A ou B, e que se deseje testar o seguinte:

$H_0$ : os habitantes da ilha são descendentes da civilização A.

$H_1$ : os habitantes da ilha são descendentes da civilização B.

Para efetuar esse teste será retirada uma amostra aleatória simples de 100 adultos dessa ilha. A regra de decisão do teste acima será a seguinte. A hipótese nula  $H_0$  será aceita se  $\bar{x} \leq t$  e será rejeitada se  $\bar{x} > t$ , em que  $\bar{x}$  representa a altura média da amostra e  $t$  é um valor crítico que depende do nível de significância do teste. Com base nessas informações, e considerando, ainda, que  $\Phi(1,645) = 0,95$ , em que  $\Phi$  representa a função de distribuição acumulada da normal padrão, julgue os itens subsecutivos.

113 Na situação em que a probabilidade de se cometer o erro do tipo I seja igual à probabilidade de se cometer o erro do tipo II, é correto afirmar que  $t = 177,7$ .

114 Para  $t = 178$  cm, a probabilidade  $\alpha$  de se cometer o erro do tipo I será menor que a probabilidade  $\beta$  de se cometer o erro do tipo II.

Considerando a matriz  $A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 0 & 2 \\ 3 & 4 & 5 \end{pmatrix}$  e os vetores  $\mathbf{x} = \begin{pmatrix} x & 1 \\ x & 2 \\ x & 3 \end{pmatrix}$  e

$\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$ , julgue os itens a seguir.

115 A matriz  $A$  tem posto 2.

116 O determinante de  $A$  é igual a  $-1$ .

117 Para que o sistema  $A\mathbf{x} = \mathbf{b}$  tenha uma solução é necessário que  $b_3 = 2b_1 + \frac{b_2}{2}$ .

Considerando a aplicação linear  $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$  dada por

$f(x, y, z) = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 4 & 2 \\ -2 & 1 & -5 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ , julgue os seguintes itens.

118 A imagem da aplicação  $f$  é a soma direta dos espaços vetoriais gerados pelos vetores  $\mathbf{v} = (11, 27, -7)$  e  $\mathbf{u} = (5, 7, 10)$ , respectivamente.

119 O núcleo de  $f$  é a reta dada por  $\{(-2t, -t, t) \mid t \in \mathbb{R}\}$ .

120 A imagem da aplicação linear  $f$  é o plano dado pela equação  $-11x + 5y + 2z = 0$ .

121 A aplicação  $f$  é injetora e não é sobrejetora.

Julgue os itens a seguir, considerando que  $V$  é o espaço vetorial de todas as funções  $f: \mathbb{R} \rightarrow \mathbb{R}$ .

RASCUNHO

122 O conjunto  $U = \{f \in V \mid f(x) \text{ é diferenciável e } f'(0) = 1\}$  é um subespaço vetorial de  $V$ .

123 O conjunto  $U = \{f \in V \mid f(x) = a + b\sin(x) + c\cos(x); a, b, c \in \mathbb{R}\}$  é um subespaço vetorial de  $V$ .

Considerando que  $M$  seja o conjunto das matrizes  $2 \times 2$ , com elementos reais, e que, para a matriz  $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M$ ,

$tr(A) = a_{11} + a_{22}$  é o traço dessa matriz, julgue os itens subsequentes.

124 O conjunto de matrizes  $U = \{A \in M \mid A \text{ não tem inversa}\}$  é um subespaço vetorial de  $M$ .

125 O conjunto de matrizes  $U = \{A \in M \mid tr(A) = 0\}$  é um subespaço vetorial de  $M$ .

Para dificultar o acesso de pessoas não autorizadas aos arquivos de determinada instituição, procedeu-se à proteção desses arquivos com senhas compostas por 3 letras minúsculas escolhidas entre as 24 primeiras letras do alfabeto, seguidas de 6 dígitos escolhidos entre os algarismos de 0 a 9. Além dessa senha de arquivo, é necessário, para o acesso a documentos altamente sigilosos, que três dos sete diretores da instituição digitem, cada um deles, sua senha pessoal.

Considerando a situação hipotética acima, julgue os itens a seguir.

126 Suponha que um *hacker* tenha descoberto que cada senha de arquivo dessa instituição era constituída por letras distintas e dígitos diferentes. Nessa situação, o referido *hacker* precisaria testar, no máximo,  $(24! \times 10!)/(21! \times 4!)$  senhas para descobrir a senha de um dos arquivos.

127 O número de maneiras de se escolherem três diretores da instituição para digitar suas senhas pessoais para abrir um arquivo altamente sigiloso é igual a 210.

128 Considere que um *hacker* tenha elaborado um *software* para descobrir a senha dos referidos arquivos e que esse *software* teste 1.000 senhas por segundo. Nessas condições, 150 dias é o tempo máximo necessário para se descobrir a senha de qualquer um dos arquivos da instituição.

Considere uma função proposicional  $P(n)$  relativa aos números naturais que satisfaça às seguintes propriedades:

- (i)  $P(3)$  é verdadeira;
- (ii) se, para um número natural  $n$ ,  $P(n)$  for verdadeira, então  $P(n^2)$  também será verdadeira;
- (iii) se, para um número natural  $n \geq 2$ ,  $P(n)$  for verdadeira, então  $P(n-1)$  também será verdadeira.

Sabendo que o conjunto dos números naturais é dado por  $\{1, 2, 3, 4, \dots\}$ , julgue os itens que se seguem, acerca de  $P(n)$  e suas propriedades.

**129** A função proposicional “a raiz quadrada de  $n$  é um número inteiro” não pode ser usada como exemplo para  $P(n)$ .

**130**  $P(n)$  é verdadeira para todos os números naturais.

### Texto para os itens de 131 a 137

Atualmente, o RSA constitui o método de criptografia com chave pública mais utilizado em aplicações comerciais. Para a implementação desse método, é preciso escolher dois números primos,  $p$  e  $q$ , e um número inteiro positivo  $c$  que seja inversível em relação à operação de multiplicação módulo  $\phi(n)$ , em que  $n = pq$  e  $\phi$  é a função de Euler que retorna a quantidade de números inteiros positivos menores que  $n$  e relativamente primos com  $n$ . A chave de codificação pública é formada por  $n$  e  $c$ . A chave de decodificação é formada por  $n$  e  $d$  — o inverso de  $c$  módulo  $\phi(n)$ . Os números  $p$ ,  $q$  e  $d$  devem ser mantidos sob segredo. A segurança do método depende de uma escolha adequada dos números primos  $p$  e  $q$  que torne o mais difícil possível a descoberta do número  $d$ , que compõe a chave de decodificação.

Considerando o texto acima e as propriedades das estruturas algébricas conhecidas como anéis, julgue os itens subsequentes.

**131** O inverso multiplicativo de  $c$  no anel dos inteiros módulo  $\phi(n)$  pode ser obtido a partir da solução da equação diofantina  $cx + \phi(n)y = 1$ , nas incógnitas  $x$  e  $y$ .

**132** Se os números primos  $p$  e  $q$  escolhidos produzirem um número  $n$  muito grande, então haverá uma quantidade muito grande de pares de números primos cujo produto também é igual a  $n$ . Por esse motivo, é muito difícil que alguém descubra os valores de  $p$  e  $q$  e, a partir deles, a chave de decodificação, o que garante a segurança do método RSA.

Considerando as informações do texto e as escolhas  $p = 5$  e  $q = 11$ , julgue os itens seguintes.

**133** Se os números  $n = 55$  e  $c = 7$  formam uma chave de codificação para o método RSA, então a chave de decodificação será formada pelos números  $n = 55$  e  $d = 23$ .

**134** O número  $c = 6$  é uma escolha apropriada para compor, juntamente com  $n = 55$ , uma chave de codificação para o método RSA.

Uma versão simplificada do processo de codificação e de decodificação RSA é apresentada a seguir.

**Etapa 1 – Pré-codificação** (converte a mensagem em uma sequência de números)

*Passo 1.* Converta cada letra da mensagem em um número, segundo a tabela abaixo, substituindo o espaço entre as palavras pelo número 99 e desconsiderando os acentos.

*Passo 2.* Divida a sequência de dígitos produzida no passo 1 em blocos disjuntos, de modo que cada bloco  $b$  seja um número menor que  $n$  e não iniciado por zero.

**Etapa 2 – Codificação:** para cada bloco  $b$  obtido no passo 2 da etapa 1, calcule o bloco codificado  $a$  da seguinte forma:  $a = C(b) = \text{resto da divisão euclidiana de } b^c \text{ por } n$ .

**Etapa 3. Decodificação:** para cada bloco  $a$  da mensagem codificada, calcule o bloco decodificado  $\hat{b}$  da seguinte forma:  $\hat{b} = D(a) = \text{resto da divisão euclidiana de } a^d \text{ por } n$ .

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

Considerando as informações do texto,  $p = 5$  e  $q = 11$ , e, ainda, o processo acima descrito, julgue os próximos itens.

**135** Se  $c = 3$ , então a mensagem PAZ será codificada na sequência de dígitos 051030.

**136** A função de decodificação  $D$  especificada na etapa 3 não realiza uma decodificação confiável, uma vez que  $\hat{b} = D(C(b))$  pode ser um bloco de dígitos diferente de  $b$ .

**137** Após o primeiro passo da etapa de pré-codificação do processo acima, a mensagem ESPIONAR É PRECISO será convertida no número 14282518242310271425271412182824.

Considere que os símbolos  $\oplus$  e  $\otimes$  representem operações sobre o conjunto dos números racionais, definidas pelas fórmulas  $a \oplus b = a + b - 1$  e  $a \otimes b = a + b - a \times b$ , em que  $a$  e  $b$  são números racionais, e os símbolos  $+$ ,  $-$  e  $\times$  representam as operações comuns de adição e de multiplicação, respectivamente. Considere, ainda, que as operações  $\oplus$  e  $\otimes$  determinam uma estrutura de corpo sobre o conjunto dos números racionais. Com base nessas informações, julgue os itens a seguir.

**138** O elemento simétrico do número 3 em relação à operação  $\oplus$  é o número  $-1$ .

**139** A equação  $(2 \otimes x) \oplus 7 = 8$  tem como única solução no conjunto dos racionais o número 1.

**140** O elemento neutro da operação  $\otimes$  é o número zero.

Considere que a variável aleatória  $X$  possa assumir  $n$  valores diferentes com probabilidades  $p_1, p_2, \dots, p_n$ , respectivamente, em que  $n \geq 2$ . A respeito das expressões das entropias de ordem  $q$  de Shannon e de Rényi associadas a  $X$ , e sabendo que ambas utilizam o logaritmo neperiano, julgue os itens a seguir.

- 141 Se todas as probabilidades  $p_i$  ( $i = 1, \dots, n$ ) forem iguais, então a entropia de Shannon e a entropia de Rényi serão iguais a  $\ln(n)$ , para qualquer valor de  $q$ .
- 142 Nessas condições, a entropia de Rényi será igual à de Shannon sempre que  $q$  for um número inteiro positivo.
- 143 Diferentemente da entropia de Rényi, a entropia de Shannon atinge o seu máximo valor quando todas as probabilidades  $p_i$  ( $i=1, \dots, n$ ) são iguais.

Determinado código utiliza um alfabeto formado por  $n$  letras diferentes  $A_1, A_2, \dots, A_n$  e as mensagens escritas nesse código são sequências finitas dessas letras. A probabilidade de aparecimento da letra  $A_i$  ( $i = 1, \dots, n$ ) nessas mensagens é dada por  $p_i$  ( $i = 1, \dots, n$ ), sendo  $p_1 + p_2 + \dots + p_n = 1$ . Portanto, se  $I(A_i)$  representa uma medida da quantidade de informação associada à letra  $A_i$ , a entropia  $H$  desse código é definida como uma média ponderada das medidas  $I(A_1), \dots, I(A_n)$ , cujos pesos são as respectivas probabilidades  $p_i$ .

Com base nas informações acima, julgue os itens seguintes, considerando o conjunto das possíveis representações binárias (sequências finitas de dígitos zeros e uns) inequívocas que podem ser associadas às letras deste código.

- 144 Considere que  $H$  seja a entropia de Shannon e que  $I(A_i) = -\log_2(p_i)$ . Nessas condições, se a taxa de transmissão por um canal for de  $R$  bits por segundo, a taxa média de transmissão de letras do código não poderá ser superior a  $\frac{R}{H}$  letras por segundo.
- 145 Se as probabilidades  $p_i$  ( $i = 1, \dots, n$ ) forem todas iguais, então a quantidade média de bits requerida para representar cada letra do código será, no mínimo,  $2\log_2(n)$  bits.
- 146 Nesse caso,  $H = p_1 I(A_1) + p_2 I(A_2) + \dots + p_n I(A_n)$ .
- 147 Assumindo-se que  $I(A_i) = -\log_2(p_i)$ , é correto afirmar que é possível construir representações binárias desse código utilizando-se, em média, menos de  $H$  bits por letra.
- 148 Se, nas mensagens geradas, cada par de letras consecutivas  $A_i A_j$  ( $i, j = 1, \dots, n$ ) for considerado como um único símbolo, a entropia de Shannon associada a esses símbolos será o dobro da entropia de Shannon associada às letras  $A_i$  ( $i = 1, \dots, n$ ).

Considere que as variáveis aleatórias  $X$  e  $Y$ , dependentes de determinado parâmetro  $R$ , sejam mutuamente independentes e que  $I_X(R)$  e  $I_Y(R)$  sejam as medidas de quantidade de informação de Fisher associadas a  $X$  e  $Y$ , respectivamente. Considere, ainda, que  $I_{X,Y}(R)$  seja a medida conjunta correspondente. A respeito dessas medidas, julgue os próximos.

- 149 A medida conjunta  $I_{X,Y}(R)$  pode ser maior que a soma  $I_X(R) + I_Y(R)$ , dependendo das distribuições de probabilidade de  $X$  e  $Y$ .
- 150 Se a variável aleatória  $X$  assumir apenas os valores 0 e 1 – considerando-se que a probabilidade de ela assumir o valor 0 seja igual a  $R$  –, então a incerteza de Fisher associada a  $n$  realizações independentes de  $X$  será  $I_X(R) = n/[R(1 - R)]$ .

RASCUNHO

## PROVA DISCURSIVA

- Nesta prova, faça o que se pede, usando o espaço para rascunho indicado no presente caderno. Em seguida, transcreva o texto para a **FOLHA DE TEXTO DEFINITIVO DA PROVA DISCURSIVA**, no local apropriado, pois **não serão avaliados fragmentos de texto escritos em locais indevidos**.
- Qualquer fragmento de texto além da extensão máxima de linhas disponibilizadas será desconsiderado.
- Na **folha de texto definitivo**, identifique-se apenas no cabeçalho da primeira página, pois não será avaliado texto que tenha assinatura ou marca identificadora fora do local apropriado.

Considere que  $X$  seja uma variável aleatória discreta que assume os valores  $x_1, \dots, x_n$  com as probabilidades  $p_1, \dots, p_n$ , respectivamente, e que, para essa variável  $X$ , a entropia seja definida como  $H(X) = -\sum_{i=1}^n p_i \ln(p_i)$ , em que  $p_i \ln(p_i) \equiv 0$  se  $p_i = 0$ . Considere, ainda, que, se  $X$  for uma variável aleatória contínua com função de densidade  $f(x)$ , a entropia será dada por  $H(X) = -\int_{-\infty}^{+\infty} f(x) \ln[f(x)] dx$ , em que  $f(x) \ln[f(x)] \equiv 0$  se  $f(x) = 0$ .  $H(X)$  é uma medida de incerteza que está relacionada com a variância da distribuição. Assim, por exemplo, se  $X$  seguir uma distribuição exponencial com variância  $\nu^2$ , a entropia correspondente será  $H(X) = 1 + \frac{1}{2} \ln \nu^2$ .

Y. Wei. Variance, entropy and uncertainty measure. In: Proceedings of the Survey Research Methods Section, p. 609-10, American Statistical Association, 1987 (com adaptações).

Com base nas informações acima descritas, redija um texto que atenda as seguintes determinações:

- ▶ determine a entropia de uma distribuição uniforme contínua no intervalo  $[a, b]$ , em que  $a < b$ ;
- ▶ enumere dois métodos para a estimação de  $H(X)$  a partir de uma amostra aleatória simples retirada de uma distribuição contínua;
- ▶ explique o significado de  $H(X) < 0$  em que  $X$  é uma variável aleatória contínua;
- ▶ explique o significado de  $H(X) = 0$ , em que  $X$  é uma variável aleatória discreta.

**RASCUNHO**

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	