Elementos de Matemática Finita

Exame - 03/02/2021

Atenção: justifique cuidadosamente todas as respostas

Cada pergunta tem a cotação de 2 valores. O exame consiste em três perguntas de cada grupo mais uma à escolha.

I

1. Dois inteiros a e b satisfazem

$$m.d.c.(a, 72) = 12, \qquad m.d.c.(b, 108) = 18.$$

Usando o Teorema Fundamental da Aritética, determinar

$$m.d.c.(ab, 144), \qquad m.d.c.(a + b, 144).$$

Resolução : Notamos que todos os inteiros presentes $(12, 18, 72,,$ etc.) são produtos de potências de 2 e de 3.
Por outro lado,

$$a = \prod_p p^{k_p}, \qquad b = \prod_p p^{j_p},$$

onde os produtos são sobre todos os primos p , e os expoentes são nulos excepto para um número finito de factores.
Sabemos que se

$$x = \prod_p p^{i_p}, \qquad y = \prod_p p^{l_p},$$

então $m.d.c.(x, y) = \prod_p p^{\min(i_p, l_p)}$.
Temos assim

$$12 = 2^2 \times 3 = m.d.c.(a, 72) = 2^{\min(k_2, 3)} \times 3^{\min(k_3, 2)},$$

e portanto $k_2 = 2$ e $k_3 = 1$, ou seja $a = 2^2 \times 3 \times u$, onde u é primo com 2 e 3.
Do mesmo modo se conclui que $b = 2 \times 3^2 \times v$, com v primo com 2 e 3.
Portanto $ab = 2^3 \times 3^3 \times u \times v$, e

$$m.d.c.(ab, 144) = 2^3 \times 3^2 = 72.$$

Evidentemente, $m.d.c(a+b, 144) = 2^i \times 3^l$, em que $0 \leq i \leq 4$ e $0 \leq l \leq 2$. 2×3 divide $a+b$ e 144; mas $2^2 \times 3$ não divide $a+b$ porque, como divide a, então dividiria b, o que é falso; e do mesmo modo 2×3^2 não pode dividir $a+b$.
Conclui-se que $m.d.c.(a+b, 144) = 6$.

2. Determinar um par de inteiros positivos ímpares consecutivos tais que

- a divisão do menor deles por 9 tem resto 3,

- o maior é múltiplo de 11

- e a soma dos dois é solução da equação $x^5 \equiv 4 \mod 13$.

Resolução : Vamos designar os dois inteiros pedidos por $2x-1$ e $2x+1$. Temos então sistema de equações modulares

$$\begin{cases} 2x - 1 \equiv 3 \mod 9 \\ 2x + 1 \equiv 0 \mod 11 \\ (4x)^5 \equiv 4 \mod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 \mod 9 \\ x \equiv 5 \mod 11 \\ x^5 \equiv 3 \mod 13 \end{cases}$$

Como 3 é primo com 13 e $5 \times 5 = 1 + 2 \times \phi(12)$, o Teorema de Fermat implica que a última equação tem solução

$$x \equiv 3^5 \equiv 9 \mod 13.$$

Se $x = 9 + 13y$, obtemos na segunda equação

$$9 + 13y \equiv 5 \mod 11 \Leftrightarrow y \equiv -2 \mod 11;$$

portanto $x = 9 + 13(-2 + 11z) = -17 + 143z$, e a primeira equação fica

$$143z \equiv 1 \mod 9 \Leftrightarrow z \equiv 8 \mod 9,$$

ou seja $x = -17 + 143(8 + 9w) = 1127 + 1287w$. Pelo Teorema Chinês dos Restos, a solução única módulo $1287 = 9 \times 11 \times 13$ do sistema é $x \equiv 1127$. Portanto dois inteiros satisfazendo as condições do enunciado são

$$2x - 1 = 2253 \text{ e } 2x + 1 = 2255.$$

3. Sendo ϕ a função de Euler, justificar que $\phi(n) \equiv 2 \mod 4$ se e só se $n = p^k$ ou $n = 2p^k$, onde p é um primo satisfazendo a condição $p \equiv 3 \mod 4$, ou se $n = 4$.

Nota: O caso $n = 4$ não foi, por lapso, mencionado no enunciado original.

Resolução : Em primeiro lugar,

$$\phi(p^k) = \phi(2p^k) = p^{k-1}(p-1).$$

Se $p \equiv 3 \mod 4$, $p - 1 \equiv 2 \mod 4$; por outro lado, p^{k-1} é congruente com 1 ou com 3 módulo 4 (conforme k é ímpar ou par), e portanto, em qualquer caso, $p^{k-1}(p-1) \equiv 2 \mod 4$. Evidentemente, $\phi(4) = 2$.
Suponhamos que n não é daquela forma. Se $n = 2^t$, com $t > 2$, $\phi(2^t) = 2^{t-1} \equiv 0 \mod 4$. Seja $n = 2^t \times m$, com $m > 1$ ímpar. Se $m = \prod_i p_i^{k_i}$, onde p_i são primos ímpares e k_i inteiros positivos,

$$\phi(n) = 2^{t-1} \prod_i p_i^{k_i - 1}(p_i - 1);$$

cada factor $p_i - 1$ contribui com uma potência positiva de 2 para $\phi(n)$; concluímos que, se $t > 1$ ou m for divisível por pelo menos dois primos distintos (ou ambos), $\phi(n) \equiv 0 \mod 4$.
O único caso não considerado ainda é $n = p^k$ ou $n = 2p^k$ com p primo, $p \equiv 1 \mod 4$; mas nesse caso

$$\phi(n) = p^{k-1}(p-1) \equiv 0 \mod 4.$$

4. Determinar, para $p > 3$ primo ímpar, em função da classe de p módulo 6 e de k,

a) quantas soluções tem a equação modular $x^6 \equiv 1 \mod p^k$;

b) para quantas classes a módulo p^k a equação $x^6 \equiv a \mod p^k$ tem solução.

Nota: Na alínea b) referia-se, por lapso, a classe de a módulo p. Isto não faria rigorosamente sentido, uma vez que, mesmo no caso em que a é primo com p^k, a existência de solução não é determinada pela classe de a módulo p. Apresenta-se a solução para o enunciado corrigido, embora na correcção dos exames se tenha tido em conta o lapso.

Resolução : p^k tem raizes primitivas e podemos aplicar o Critério de Euler. A equação da alínea a) tem d soluções, onde

$$d = m.d.c.(6, \phi(p^k)) = m.d.c.(6, p^{k-1}(p-1)) =$$

$$m.d.c.(6, p-1) = \begin{cases} 6 & \text{se } p \equiv 1 \mod 6 \\ 2 & \text{se } p \equiv 5 \mod 6 \end{cases}$$

Na alínea b), se a for primo com o módulo, a equação tem d soluções se $a^{\frac{\phi(p^k)}{d}} \equiv 1 \mod p^k$, e nenhuma caso contrário. Escrevendo $a \equiv g^y$, com g raiz primitiva e $0 \leq y < p^{k-1}(p-1)$, vemos que existem soluções se e só se $y \equiv 0 \mod d$, ou seja, para $\frac{p^{k-1}(p-1)}{d}$ classes a primas com o módulo.
Resta considerar o caso em que a classe a não é prima com o módulo. Esta é a parte mais difícil do problema.
Se $a \equiv 0$, existe sempre solução; caso contrário, podemos representar a por $p^j b$ onde $1 \leq j < k$ e b primo com p^k. Note-se que esta representação não é única: se $a \equiv p^j b \mod p^k$ como descrito, j fica determinado pela classe de a (p^j é o máximo divisor comum entre qualquer representante da classe a e p^k), mas existem p^j classes b módulo p^k, primas com este, distintas, satisfazendo a congruência (fixando b, $a \equiv p^j(b + tp^{k-j})$, para todo o $0 \leq t < p^j$); ou seja a é determinado por j e pela classe de b módulo p^{k-j}.
Uma solução da equação $x^6 \equiv p^j b \mod p^k$ terá que ser da forma $x \equiv p^i u$, com $6i = j$ e $u^6 \equiv b \mod p^{k-j}$. A existência de solução desta última congruência não depende da classe b usada na representação $a \equiv p^j b \mod p^k$. Como b é primo

com p^{k-j}, podemos aplicar o critério de Euler: mais uma vez, $m.d.c.(6, \phi(p^{k-j})) = m.d.c.(6, p-1) = d$, determinado no início; e a equação tem solução se

$$b^{\frac{\phi(p^{k-j})}{d}} \equiv 1 \mod p^{k-j},$$

ou seja, repetindo o raciocínio feito anteriormente, para $\frac{\phi(p^{k-j})}{d}$ classes. O caso inicial (a primo com p^k) está contido neste, pondo $j = 0$.
Em resumo, a equação $x^6 \equiv a \mod p^k$ tem solução para

$$1 + \sum \frac{\phi(p^{k-j})}{d}$$

classes, onde a soma é sobre os inteiros $0 \leq j < k$, tais que $j \equiv 0 \mod 6$, e d é determinado pela classe de p módulo 6, como descrito na alínea a).

II

Nota: Recordar que, dada uma função $f : X \to Y$, e $S \subset Y$, a imagem inversa de S por f é

$$f^{-1}(S) = \{x \in X : f(x) \in S\}\}.$$

Recordar também que $[n] = \{u \in \mathbb{Z},\ 0 \leq u < n\}$.
Nos exercícios **5.** e **6.**, $S \subset [30]$ é um conjunto fixo com 10 elementos.

5.

a) Determinar o número de funções $f : [100] \to [30]$ que satisfazem a condição $f^{-1}(S) \neq \emptyset$.

b) Determinar o número de funções $f : [100] \to [30]$ que satisfazem a condição $|f^{-1}(y)| = 3$ para todo o $y \in S$.

Resolução : Existem 20^{100} funções $f : [100] \to [30]$ tais que $f^{-1}(S) = \emptyset$. Portanto a resposta de a) é $30^{100} - 20^{100}$.

Na alínea b) temos que escolher três pré-imagens para cada $y \in S$, sendo a imagem de cada um dos restantes elementos de $[100]$ qualquer $u \in [30] \setminus S$. A resposta é

$$\frac{100!}{(3!)^{10}70!}20^{70}.$$

6. Determinar o número de funções $f : [100] \to [30]$ que satisfazem a condição $f^{-1}(y) \neq \emptyset$ para todo o $y \in S$.

Resolução : Usamos o Princípio de Inclusão-Exclusão: sendo, para cada $y \in S$, U_y o conjunto de funções $f : [100] \to [30]$ tais que $f^{-1}(y) = \emptyset$, queremos calcular $30^{100} - |\cup_y U_y|$.
para qualquer subconjunto $\{y_1, \cdots, y_j\} \subset S$

$$U_{y_1} \cap \cdots U_{y_j} = (30-j)^{100},$$

e portanto

$$30^{100} - |\cup_y U_y| = 30^{100} - \sum_{j=1}^{10}(-1)^{j-1}\binom{10}{j}(30-j)^{100}.$$

7. Determinar o número de funções $f : [100] \to [30]$, não decrescentes (isto é, $f(k+1) \geq f(k)$, para todo o k) que satisfazem a condição $f(0) = 0$.
Sugestão : considerar $y_k = f(k+1) - f(k)$.

Resolução : Determinar uma função nas condições do enunciado é equivalente a escolher a sequência $y_k = f(k+1) - f(k)$, $0 \leq k < 100$, em que $0 \leq y_k$ e

$$\sum_{k=0}^{98} y_k = f(99) - f(0) \leq 29.$$

O número de soluções é igual ao de

$$\sum_{k=0}^{99} y_k = 29, \qquad 0 \leq y_k,$$

que é $\binom{128}{29}$.

8. No conjunto das funções $f : [n] \to [k]$ definimos a seguinte relação de equivalência: $f \sim g$ se existe uma permutação $\pi \in S_n$ tal que $g = f \circ \pi$.
Usar a contagem de classes de equivalência para deduzir que

$$\frac{1}{n!}\sum_{j=1}^{n} c(n,j)k^j = \binom{n+k-1}{n},$$

onde $c(n,j)$ são números de Stirling de primeira espécie.

Nota: Por lapso, no enunciado original não foi incluído o factor $\frac{1}{n!}$. Esse facto foi tido em conta na correcção .

Resolução : A relação de equivalência definida pode ser traduzida pela propriedade de duas funções f e g serem equivalentes se e só se

$$|f^{-1}(y)| = |g^{-1}(y)|, \ \forall y \in [k].$$

Logo há $\binom{n+k-1}{n}$ classes de equivalência.
Por outro lado, aplicando o Teorema de Cauchy-Frobenius-Burnside, o número de classes de equivalência é

$$\frac{1}{n!}\sum_{\pi \in S_n} |I(\pi)|.$$

Ora $f \in I(\pi)$ siginifica que $f \circ \pi(x) = f(x)$, para todo o $x \in [n]$, ou seja, que f é constante em cada ciclo de π. Portanto $|I(\pi)| = k^j$ onde j é o número de ciclos da permutação. Como há $c(n,j)$ permutações com j ciclos, temos o resultado.

III

9. G é um grafo simples com 22 arestas, em que cada vértice v satisfaz $3 \leq d(v) \leq 4$.

a) Determinar os possíveis números de vértices de cada grau.

b) G pode ter um passeio Euleriano?

Resolução : Se G tem x vértices de grau 3 e y vértices de grau 4, temos

$$3x + 4y = 44 \Leftrightarrow x = -44 + 4k \wedge y = 44 - 3k,\ k \in \mathbb{Z}.$$

Como x e y são não negativos, temos necessariamente $3k \leq 44 \leq 4k$, ou seja $11 \leq k \leq 14$.
Portanto os possíveis valores são

$$x = 0, y = 11 \text{ ou } x = 4, y = 8 \text{ ou } x = 8, y = 5 \text{ ou } x = 12, y = 2.$$

Verifica-se que as sequências de graus determinadas por estes valores são todas admissíveis.
G pode ter um passeio Euleriano (fechado) no primeiro caso, uma vez que todos os vértices têm grau par, desde que seja conexo. E prova-se facilmente que existe um grafo conexo com 11 vértices, regular de grau 4. De facto, prova-se por indução que para todo o $n \geq 5$ existe um grafo conexo com n vértices, regular de grau 4: para $n = 5$ é o grafo completo K_5; assumindo que G, conexo e regular de grau 4, tem $n-1$ vértices ($n > 5$), tomamos dois pares de vértices adjacentes, eliminamos as duas arestas que os unem e ligamos esses 4 vértices a um novo véertice; a regularidade e a conectividade do grafo é preservada.

10. Seja G um grafo simples, conexo e planar, com 13 vértices. Uma representação plana de G tem 11 faces, 5 de grau 4, 4 de grau 3 e 2 de grau t.

a) Calcular t e o número de arestas de G.

b) Justificar que o grau mínimo de G satisfaz $\delta(G) \leq 3$ e que se $\delta(G) = 3$, então G tem pelo menos 6 vértices de grau mínimo.

Resolução : A fórmula de Euler implica imediatamente que G tem $13+11-2 = 22$ arestas. Como a soma dos graus das faces iguala o dobro do número das arestas, temos

$$5 \times 4 + 4 \times 3 + 2 \times t = 44 \Leftrightarrow t = 6.$$

A fórmula $\sum_v d(v) = 44$ implica imediatamente que $\delta(G) \leq 3$. E se tivermos igualdade e G tiver exactamente s vértices de grau 3

$$3s + 4(13 - s) \leq 44 \Leftrightarrow 8 \leq s.$$

Nota: um erro de contas levou ao valor 6 em vez de 8. Evidentemente, a dedução correcta implica também $6 \leq s$.

10. Seja G um grafo simples, conexo e planar, com k vértices de grau 4, tendo os restantes $k + 1$ vértices grau 3. As representações planas de G têm 10 faces.

a) Calcular o número de vértices e arestas de G.

b) Justificar que qualquer representação plana de G tem pelo menos 2 faces de grau 3.

Resolução : Temos, pela fórmula de Euler, $2k + 1 - a + 10 = 2 \Leftrightarrow a = 2k + 9$, e, por outro lado, $4k + 3(k + 1) = 2a$. Estas duas igualdades são equivalentes a $k = 5$ e $a = 19$, ou seja, G tem 11 vértices e 19 arestas.
Como o grau de cada face é pelo menos 3 e a soma dos graus das faces iguala o dobro do número de arestas, designando por s o número de faces de grau 3, temos

$$38 = \sum_f d(f) \geq 3s + 4(10 - s) \implies s \geq 2.$$

Nota: O enunciado da primeira alínea do problema **11.** estava errada, sendo o resultado, nos termos apresentados, falso. Em face disso, foi seguida a opção de

dar a cotação total da pergunta a todos os exames. Apresenta-se a seguir a versão corrigida, com a respectiva resolução.

11. Seja G um grafo simples, conexo com n vértices, e H um subgrafo obtido por eliminação de arestas.

a) Justificar que os polinómios de coloração $p(G,x)$ e $p(H,x)$ satisfazem a desigualdade $p(G,k) \leq p(H,k)$, para todo o inteiro positivo k.

b) Deduzir que, para todo o inteiro positivo k, $p(G,k) \leq k(k-1)^{n-1}$.

Resolução : Cada coloração de G com k cores é também uma coloração de H com k cores, logo, se G pode ser colorido com k cores de $m = p(G,k)$ maneiras, H pode também ser colorido com k cores, de pelo menos m maneiras, o que justifica a desigualdade em a).
A alínea b) decorre de G ter, uma vez que é conexo, como subgrafo com o mesmo conjunto de vértices, uma árvore geradora. O polinómio de coloração de uma árvore com n vértices é $p(T,x) = x(x-1)^{n-1}$.

12. Seja $G[X,Y]$ um grafo simples bipartido que tem um emparelhamento que cobre X.

a) Mostrar que se $x \in X$ tem um vértice adjacente $y \in Y$ tal que a aresta $x-y$ não pertence a nenhum emparelhamento máximo, então existe $S \subset X$ tal que $|N(S)| = |S|$.

b) Deduzir que existe $x \in X$ tal que, para todo o $y \in N(x)$, a aresta $x-y$ pertence a algum emparelhamento máximo.

c) Concluir que, se $|X| = m$ e $d(x) \geq d$, com $d \leq m$, então existem pelo menos $d!$ emparelhamentos máximos.

Resolução: Seja G' o subgrafo obtido eliminando os vértices x e y (e as arestas neles incidentes). Pela hipótese, G' nãtem nenhum emparelhamento que cubra $X - x$, uma vez que se o tivesse, esse emparelhamento, juntamente com a aresta

$x - y$ seria um emparelhamento máximo contendo $x - y$.
Portanto tem que existir $S \subset X - x$ (não vazio) que não satisfaça a condição do Teorema de Hall em G', ou seja, o conjunto $N'(S)$ dos vértices adjacentes a vértices de S tem que satisfazer $|N'(S)| < |S|$; por outro lado, pelo mesmo Teorema, em $G[X, Y]$ temos $|N(S)| \geq |S|$; ora $N'(S) = N(S) \cap (Y - y)$, pelo que a única possibilidade é que $N'(S) = N(S) - y$ e portanto $|N(S)| = |S|$.
Note-se que em qualquer emparelhamento de $G[X, Y]$ cobrindo X, os vértices de S são emparelhados com os de $N(S)$, e os de $X \setminus S$ com vértices de $Y \setminus N(S)$.
Podemos então provar b) por indução em X. O caso $|X| = 1$ é trivial; suponhamos para todo o grafo bipartido $G[X', Y']$ com $|X'| < n$ que tem um emparelhamento cobrindo X' existe $x \in X'$ satisfazendo a condição de b): qualquer aresta $x - y$ pertence a algum emparelhamento que cobre X'. Se $G[X, Y]$ tem um emparelhamento que cobre X e algum vértice x não satisfaz essa condição, consideramos o grafo $G[S, N(S)]$, onde $S \subset X$ é o conjunto cuja existência se provou em a), e $N(S) \subset Y$ a sua vizinhança em $G[X, Y]$. Como $|S| < |X|$, por hipótese de indução, existe $u \in S$ satisfazendo a condição do enunciado: para todo o $v \in N(u)$ (e este conjunto é o mesmo em $G[X, Y]$ e em $G[S, N(S)]$), existe um emparelhamento cobrindo S que contém a aresta $u - v$. Mas como vimos acima, este emparelhamento pode ser estendido a $G[X, Y]$.
A demonstração de c) pode ser feita por um raciocínio semelhante. Se $|X| = 1$ o resultado é mais uma vez trivial; supômos que a propriedade é válida para todos os grafos bipartidos $G[X', Y']$, com $|X'| < n$, que têm um emparelhamento cobrindo X': se existe $d' \leq |X'|$ tal que $d(x) \geq d'$ para todo o $x \in X'$, então o grafo tem pelo menos $d'!$ emparelhamentos cobrindo X'.
Seuponhamos que $G[X, Y]$ tem um emparelhamento cobrindo X, $|X| = n$ e que todos os vértices $x \in X$ satisfazem $d(x) \geq d$, para algum $d \leq m$. Escolhendo um vértice x_0 nas condições da alínea b), vemos que existe pelo menos um emparelhamento cobrindo X por cada vértice y adjacente a x_0. Para cada um desses y, se eliminarmos x_0 e y (e as arestas incidentes), obtemos um novo grafo bipartido, que tem um emparelhamento cobrindo $X - x_0$ e em que para todo o $x \in X - x_0$, $d(x) \geq d - 1$, com $d - 1 \leq |X - x_0|$. Por hipótese de indução, este grafo tem pelo menos $(d-1)!$ emparelhamentos e cada um deles pode ser estendido a $G[X, Y]$ com

a aresta $x_0 - y$. Como há pelo menos d vértices y, obtemos o resultado pretendido.