Elementos de Matemática Finita

Exame - 10/01/2020

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. Determinar (ou mostrar que não existem) todas as soluções com $x, y > 0$ da igualdade

$$23x + 13y = 1000.$$

Resolução : Por aplicação do algoritmo de Euclides temos

$$1 = 23 \times 4 - 13 \times 7 = 23 \times (4 - 13k) + 13 \times (-7 + 23k),$$

e portanto

$$1000 = 23 \times (4000 - 13k) + 13 \times (-7000 + 23k).$$

Deduzimos que as soluções pedidas são

$$x = 4000 - 13k, \qquad y = -7000 + 23k,$$

com

$$13k < 4000 \wedge 23k > 7000 \Leftrightarrow 305 \leq k \leq 307,$$

ou seja, temos os pares (x, y)

$$(35, 15),\ (22, 38),\ (9, 61).$$

2. Determinar (ou mostrar que não existem) as soluções $0 < x < 2020$ de

$$x^7 \equiv 111 \mod 2020.$$

Resolução : Como 111 ´ primo com 2020 e $2020 = 4 \times 5 \times 101$, e portanto $\phi(2020) = 2 \times 4 \times 100 = 800$ que é primo com 7, a equação tem solução única. A form mais simples de a calcular ´ provavelmente por aplicação do Teorema Chinês dos Restos:

$$x^7 \equiv 111 \mod 2020 \Leftrightarrow \begin{cases} x^7 \equiv 111 \mod 4 \\ x^7 \equiv 111 \mod 5 \\ x^7 \equiv 111 \mod 101 \end{cases}.$$

Este sistema é equivalente a

$$\begin{cases} x \equiv 3 \mod 4 \\ x^3 \equiv 1 \mod 5 \\ x^7 \equiv 10 \mod 101 \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \mod 4 \\ x \equiv 1 \mod 5 \\ x \equiv 10^{43} \mod 101 \end{cases}$$

aplicando o Teorema de Fermat. A última equação resolv-se facilmente notando que $10^2 \equiv -1 \mod 101$ e que portanto $10^{43} \equiv 10^3 \equiv -10 \mod 101$. Ficamos portanto com o sistema

$$\begin{cases} x \equiv 3 \mod 4 \\ x \equiv 1 \mod 5 \\ x \equiv -10 \mod 101 \end{cases}$$

que tem como solução $91 \mod 2020$.

3. Dado um primo ímpar e $m > 0$, sejam $g_1, \cdots, g_t$ as raizes primitivas módulo p^m. Calcular $\prod_{i=1}^{t} g_i \mod p^m$.

Resolução : Para cada i existe um (e um só) $0 < s_i < \phi(p^m)$, primo com $\phi(p^m)$, tal que $g_i \equiv g_1^{s_i}$. Portanto

$$\prod_{i=1}^{t} g_i \equiv g_1^{\sum s} \mod p^m,$$

onde o expoente é a soma de todas as classes módulo $\phi(p^m) = p^{m-1}(p-1)$ primas com este valor. Mas se s é uma dessas classes, $-s$ também o é; além disso s e $-s$ não são congruentes módulo $\phi(p^m)$, a não ser num único caso:

$$s \equiv -s \mod \phi(p^m) \implies 1 \equiv -1 \mod \phi(p^m),$$

uma vez que s é invertível módulo $\phi(p^m)$; ora esta última congruência só é verdadeira se $\phi(p^m) = 2$, ou seja, se $p = 3$ e $m = 1$.
Este caso pode ser deduzido directamente: a única raiz primitiva é 2. Em todos os outros casos, o raciocínio anterior mostra que a soma $\sum s$ das classes primas com $\phi(p^m)$ é congruente com zero e portanto $\prod_{i=1}^{t} g_i \equiv 1 \mod p^m$.

4.

a) Determinar para que valores de $m \geq 0$ é que $2^m + 1$ é resíduo quadrático mod 5.

b) Seja $m \equiv 0 \mod 4$. Mostrar que se $n = 2^m + 1$ é primo então $5^{\frac{n-1}{2}} \equiv -1 \mod n$.

c) Mostrar que a recíproca é verdadeira: se $n = 2^m + 1$, com $m \equiv 0 \mod 4$, e $5^{\frac{n-1}{2}} \equiv -1 \mod n$, então n é primo

Sugestão: na alínea c), considerar um factor primo p de n e determinar a ordem de 5 módulo p.

Resolução : Os resduos quadráticos módulo 5 são 1 e 4; por outro lado

$$2^m + 1 \equiv \begin{cases} 2 & \text{se } m \equiv 0 \mod 4 \\ 3 & \text{se } m \equiv 1 \mod 4 \\ 0 & \text{se } m \equiv 2 \mod 4 \\ 4 & \text{se } m \equiv 3 \mod 4 \end{cases}$$

portanto $2^m + 1$ é resíduo quadrático mod 5 se e só se $m \equiv 3 \mod 4$.
Se $m \equiv 0 \mod 4$ e $n = 2^m + 1$ é primo, deduzimos da Lei da Reciprocidade Quadrática que 5 não é resíduo quadrático mod n:

$$(5|n) = (n|5) = -1.$$

Mas então, pelo critério de Euler, $5^{\frac{n-1}{2}} \equiv -1 \mod n$.
Suponhamos agora que $5^{\frac{n-1}{2}} \equiv -1 \mod n$, e, seguindo a sugestão, seja p um divisor primo de n. Seja d a ordem de 5 módulo p; a hipótese implica que $5^{2^{m-1}} \equiv -1$

mod p e que $5^{2^m} \equiv 1 \mod p$, logo $d = 2^m$. Mas então $2^m \mid (p-1)$, ou seja, $p = t2^m + 1$ para algum t inteiro. Deduzimos que $p = n$ e portanto n é primo.

II

5. De quantas maneiras podemos ordenar os inteiros $\{0, 1, \cdots, 99\}$ de modo a que

a) haja o mesmo número de múltiplos de 3 nas metades inicial e final da sequência?

b) as potências de 2 fiquem por ordem crescente?

Resolução : a) Podemos escolher os múltiplos de 3 que ficarão em cada uma das metades da sequência de $\binom{34}{17}$ maneiras; do mesmo modo, escolhemos os não múltiplos de 3 para cada uma das metades de $\binom{66}{33}$ maneiras. Em seguida ordenamos os elementos de cada metade da sequência. O resultado final é portanto

$$\binom{34}{17}\binom{66}{33}50!50!.$$

Na alínea b) Escolhemos os lugares para as 7 potências de 2 e ordenamos os restantes inteiros. O resultado é

$$\binom{100}{7}93!.$$

6. Dado um conjunto de primos p_i, $1 \leq i \leq m$, seja $P = \prod_{i=1}^{m} p_i$. Determinar uma expressão para o número de divisores positivos de P^{30} que não são de nenhuma das formas x^2, x^3, x^5, x^7.

Resolução : P^{30} tem 31^m divisores positivos. Seja X_2 o conjunto dos divisores que são quadrados perfeitos, e analogamente para os divisores da forma x^3, x^5, x^7. Queremos calcular $31^m - |X_2 \cup X_3 \cup X_5 \cup X_7|$ e aplicamos o Princípio de Inclusão-Exclusão: temos

$$|X_2| = 16^m,\ |X_3| = 11^m,\ |X_5| = 7^m,\ |X_7| = 5^m;$$

$|X_2 \cap X_3| = 6^m$, $|X_2 \cap X_5| = 4^m$, $|X_2 \cap X_7| = |X_3 \cap X_5| = 3^m$, $|X_3 \cap X_7| = 2^m$, $|X_5 \cap X_7| = 1$;

$|X_2 \cap X_3 \cap X_5| = 2^m$, $|X_2 \cap X_3 \cap X_7| = |X_2 \cap X_5 \cap X_7| = |X_3 \cap X_5 \cap X_7| = 1$;

e finalmente $|X_2 \cap X_3 \cap X_5 \cap X_7| = 1$.
A expressão pedida é portanto

$$31^m - (16^m + 11^m + 7^m + 5^m) + (6^m + 4^m + 2 \times 3^m + 2^m + 1) - (2^m + 3) + 1.$$

7. Sendo S_{12} o conjunto das permutações de $[12] = \{0, 1, \cdots, 11\}$,

a) Determinar, para $k = 4$ e $k = 5$, uma fórmula para o número de permutações $\sigma \in S_{12}$ que satisfazem $\sigma^k = \iota$ (onde ι designa a permutação identidade).

b) Determinar o número de permutações $\sigma \in S_{12}$ que satisfazem $\sigma^2 = \pi$ com

$$\pi = (0, 1, 2)(3, 4, 5)(6, 7, 8)(9)(10)(11).$$

Resolução : Uma permutação $\sigma \in S_{12}$ satisfaz $\sigma^5 = \iota$ se os seus ciclos tiverem comprimento 1 ou 5. O número de permutações com j 5-ciclos e $12 - 5j$ 1-ciclos é

$$\frac{12!(4!)^j}{(5!)^j j!(12-5j)!},$$

e portanto a fórmula pedida é

$$\sum_{j=0}^{2} \frac{12!(4!)^j}{(5!)^j j!(12-5j)!} = \sum_{j=0}^{2} \frac{12!}{5^j j!(12-5j)!}.$$

No caso $\sigma^4 = \iota$, temos que considerar ciclos com comprimento 1, 2 ou 4 e a fórmula fica ligeiramente mais complicada:

$$\sum_{j=0}^{3} \sum_{k=0}^{6-2j} \frac{12!(3!)^j}{(4!)^j (2!)^k j!k!(12-4j-2k)!} = \sum_{j=0}^{3} \sum_{k=0}^{6-2j} \frac{12!}{2^{2j+k} j!k!(12-4j-2k)!}.$$

Na alínea b), uma permutação σ que satisfaz $\sigma^2 = \pi$ pode ter ciclos de comprimento 1, 2, 3 ou 6; isto porque um m-ciclo de σ dá origem a um m-ciclo de σ^2 se

m for ímpar ou a dois $\frac{m}{2}$-ciclos se m for par. Indicam-se os possíveis números de ciclos de comprimentos 1, 2, 3 e 6 que podem existir em σ:

$$\begin{array}{cccc} 3 & 0 & 3 & 0 \\ 1 & 1 & 3 & 0 \\ 3 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{array}$$

no primeiro caso existe uma única permutação satisfazendo a condição:

$$\sigma = (0,2,1)(3,5,4)(6,8,7)(9)(10)(11).$$

No segundo caso o 2-ciclo pode ser constituído por quaisquer dois dos elementos $9, 10, 11$ (de uma única maneira) e os 3-ciclos são os mesmos do caso anterior; temos portanto 3 permutações nessas condições.
No terceiro caso, podemos formar o 6 ciclo com os elementos de dois dos 3-ciclos de π, e para cada uma dessas escolhas o ciclo pode formar-se de 3 maneiras: por exemplo, se o 6 ciclo contiver os elementos $1, 2, 3, 4, 5, 6$, ele pode ser um dos seguintes

$$(1,4,2,5,3,6), \qquad (1,5,2,6,3,4), \qquad (1,6,2,4,3,5);$$

temos portanto 9 permutações σ com esse tipo cíclico que satisfazem $\sigma^2 = \pi$.
Finalmente, no quarto caso conjugamos as enumerações de ciclos feitas nos casos anteriores: existem 27 permutações nessas condições.
Conclui-se que existem no total 40 permutações que satisfazem $\sigma^2 = \pi$.

8. Seja $D(m,n)$ o número de caminhos entre $(0,0)$ e (m,n) que se podem fazer com passos $(1,0)$, $(0,1)$ e $(1,1)$.
Mostrar que $D(m,n) = \sum_k \binom{m}{k}\binom{n+k}{m}$.
Sugestão: classificar os caminhos em função do número de passos $(1,1)$ usados.

Resolução : Cada caminho contendo j passos $(1,1)$ pode ser obtido de um caminho com $m-j$ passos $(1,0)$ e $n-j$ passos $(0,1)$, intercalando em quaisquer das $m+n-2j+1$ posições resultantes os passos $(1,1)$. Logo

$$D(m,n) = \sum_j \binom{m+n-2j}{n-j}\binom{j+m+n-2j}{m+n-2j} = \sum_j \binom{m+n-j}{m+n-2j}\binom{m+n-2j}{n-j} =$$

$$= \sum_j \binom{m+n-j}{n-j} \binom{m}{(m+n-2j)-(n-j)} = \sum_j \binom{m+n-j}{m} \binom{m}{m-j},$$

e a fórmula do enunciado obtém-se substituindo $k = m - j$.

III

9. O grafo simples G tem 15 vértices e 25 arestas. t vértices têm grau k e os restantes têm grau $k+1$. Determinar k e t.
Quantas componentes conexas pode G ter?

Resolução : Temos $kt + (k+1)(15-t) = 50 \Leftrightarrow 15k - t = 35$. A única solução em inteiros $0 \leq k \leq 14$ e $0 \leq t \leq 15$ é $k = 3$, $t = 10$, e portanto G tem 10 vértices de grau 3 e 5 de grau 4.
Como o grau mínimo é 3, cada componente conexa de G tem que ter pelo menos 4 vértices, logo o número de componentes conexas tem que ser menor que 4. Vamos justificar que os valores 1, 2 e 3 são todos possíveis: para isso é útil notar que os cinco vértices de grau 4 podem formar um K_5, e lembrar que para qualquer $m \geq 4$, par, existem grafos regulares de grau 3; podemos portanto ter três componentes conexas, duas regulares de grau 3 (com 4 e 6 vértices) e a outra regular de grau 4, ou duas componentes, uma regular de grau 3 e a outra regular de grau 4.
Para ver que é também possível ter uma única componente conexa, podemos por exemplo notar que existe um grafo com 14 vértices, regular de grau 3 e que se acrescentarmos um novo vértice ligando-o a quatro dos anteriores obtemos um grafo com a distribuição de graus pedida.
Note-se que é possível também ter outros grafos com duas ou três componentes conexas, não isomorfos aos descritos acima.

10. Quantas folhas pode ter uma árvore com vértices v_i, $1 \leq i \leq 30$, em que todos os outros vértices têm grau 3 ou 4?
Determinar o número de árvores desse tipo em que as folhas são os vértices v_i com $1 \leq i \leq 20$.

Resolução : Se t for o número de vértices de grau 3 e k o número de vértices de grau 4, e $j = 30 - t - k$ o número de folhas, temos

$$4k + 3t + 30 - k - t = 58 \Leftrightarrow 3k + 2t = 28 \Leftrightarrow k = \frac{2(14-t)}{3};$$

portanto $0 \leq 14 - t$ tem que ser divisível por 3, ou seja, temos os seguintes triplos (t, k, j) possíveis:

$$(2, 8, 20), \qquad (5, 6, 19), \qquad (8, 4, 18), \qquad (11, 2, 17), \qquad (14, 0, 16).$$

As árvores referidas na segunda parte da pergunta correspondem ao primeiro caso; como as folhas estão determinadas, contamos o número de árvores escolhendo quais os vértices com grau 3 e grau 4 e, para cada uma dessas escolhas, o número de árvores com a sequência de graus assim determinada, usando o código de Prüfer: temos que escolher no código de comprimento 28, 3 posições para cada vértice de grau 4 e 2 posições para cada vértice de grau 3. O resultado final é

$$\binom{10}{2} \frac{28!}{(2!)^2 (3!)^8}.$$

11. Seja G um grafo simples com n vértices, conexo e regular de grau k. Mostrar que $\omega(G) = n$ ou $\omega(G) \leq \frac{n}{2}$.
Sugestão : considerar separadamente os casos $k \leq \frac{n}{2}$ e $k > \frac{n}{2}$. Considerar $\alpha(G)$ (acrescentado no exame).

Resolução : Seja X um conjunto independente de vértices de G com $|X| = \alpha = \alpha(G)$. Há αk arestas a ligar X a $V_G \setminus X$; por outro lado, esse número tem que ser menor ou igual a $(n - \alpha)k$, logo

$$\alpha k \leq (n - \alpha)k \Leftrightarrow \alpha \leq \frac{n}{2},$$

a menos que $k = 0$. Aplicando este raciocínio ao complementar de G, conclui-se que, ou $\overline{G}$ não tem arestas, e nesse caso $G = K_n$ e obviamente $\omega(G) = n$, ou então

$$\omega(G) = \alpha(\overline{G}) \leq \frac{n}{2}.$$

12. Suponhamos que os vértices do grafo G se podem decompor numa união disjunta $V = A \cup B$ de tal modo que os subgrafos induzidos $G[A]$ e $G[B]$ têm

número de coloração m, e que o número de arestas entre A e B é menor que m. Mostrar que então $\chi(G) = m$.

Resolução : As condições implicam imediatamente que $\chi(G) \geq \chi(G[A]) = m$. Consideremos decomposições

$$A = \bigcup_{1 \leq i \leq m} X_i, \qquad B = \bigcup_{1 \leq j \leq m} Y_j$$

como uniões disjuntas em conjuntos estáveis. Se existir uma bijecção $\pi : \{1, \cdots, m\} \to \{1, \cdots, m\}$ tal que, para todo o i, $X_i \cup Y_{\pi(i)}$ é estável, conclui-se que $\chi(G) = m$.
Se definirmos o grafo bipartido $H[I, J]$ onde $I = J = \{1, \cdots, m\}$ e existe uma aresta incidente em i e j se e só se $X_i \cup Y_j$ é estável, queremos mostrar que $H[I, J]$ tem um emparelhamento perfeito. Aplicamos o Teorema de Hall para deduzir que existe um emparelhamento cobrindo I: dados

$$S = \{i_1, \cdots, i_l\} \subset I, \qquad N(S) = \{j_1, \cdots, j_k\},$$

onde $N(S)$ designa o conjunto de vértices adjacentes a algum $i_t \in S$, queremos mostrar que $l \leq k$.
A definição de $H[I, J]$ implica que para todo o $1 \leq t \leq l$ e todo o $j \in \{1, \cdots, m\} \setminus N(S)$, existem $x \in X_{i_t}$ e $y \in Y_j$ adjacentes em G; pela hipótese, temos $l(m-k) < m$ ou seja $l(m-k) \leq m-1$; se $l > k$, então $l(m-l) < l(m-k) \leq m-1$, e portanto $m(l-1) < l^2 - 1$. Esta desigualdade implica imediatamente que $l > 1$ e fica equivalente a $m < l + 1$, ou seja, a $l = m$. Mas então a desigualdade com que começámos este raciocínio fica

$$m(m-k) \leq m-1 \Leftrightarrow m - 1 + \frac{1}{m} \leq k,$$

e portanto $l = m \leq k \leq m$ contradizendo a possibilidade $l > k$.
Conclui-se que para todo o $S \subset I$, $|S| \leq |N(S)|$ e portanto existe um emparelhamento perfeito, como queríamos provar.