

Elementos de Matemática Finita

Ficha Complementar: o problema de Frobenius

Dado um conjunto de inteiros positivos

$$A = \{a_1 < a_2 < \dots < a_n : m.d.c. (a_1, a_2, \dots, a_n) = 1\}$$

diz-se que um inteiro x é **representável** (ou, mais explicitamente, representável por $\{a_1, a_2, \dots, a_n\}$) se existirem inteiros *não negativos* u_1, u_2, \dots, u_n tais que

$$x = u_1 a_1 + u_2 a_2 + \dots + u_n a_n.$$

O Problema de Frobenius consiste em, dados os a_i , encontrar o maior inteiro que *não é* representável e que denotamos por $g(a_1, a_2, \dots, a_n)$.

Porque que deveria existir este número? A dúvida é perfeitamente razoável mas a sua existência ser confirmada mais à frente.

0. Se $\min\{a_i : 1 \leq i \leq n\} = 1$, qual o valor de $g(a_1, a_2, \dots, a_n)$?

1. Considerar $A = \{2, 5\}$ e verificar que todos os inteiros excepto 1 e 3 são representáveis. Portanto, que neste caso $g(2, 5) = 3$;

2. Considerar agora $A = \{5, 7\}$ e deduzir que $g(5, 7) = 23$;

3. Demonstrar que para $n = 2$ se tem a seguinte *fórmula de Sylvester*

$$g(a, b) = (a - 1)(b - 1) - 1.$$

Sugestão: qualquer inteiro x se pode escrever, de uma única maneira, na forma

$$x = au + bv$$

com $0 \leq u < b$ (porquê?).

Justificar que se x é representável por $\{a, b\}$ então esta é uma das possíveis representações. Qual o maior $x = au + bv$ para o qual $0 \leq u < b$ e $v < 0$?

4. Uma dedução ligeiramente diferente da fórmula de Sylvester, usando mais explicitamente a noção de congruência:

- a) Justificar que em cada classe de congruência módulo a o menor inteiro representável é um múltiplo de b , mais especificamente, mostrar que se, para cada $0 \leq t < a$, definirmos m_t como o menor inteiro representável por $\{a, b\}$ e congruente com t módulo a , então $m_t = bv_t$ onde v_t é o único inteiro que satisfaz

$$0 \leq v_t < a \quad bv_t \equiv t \pmod{a}.$$

- b) Notar que as classes de congruência módulo a de bu , com $0 \leq u < a$, são todas distintas.
- c) Concluir que a classe de congruência módulo a de $g(a, b)$ tem que ser a mesma de $b(a - 1)$ e que, portanto,

$$g(a, b) = b(a - 1) - a.$$

5. Mostrar que, dados $0 < a < b$, os conjuntos dos inteiros representáveis e dos não representáveis são mutuamente simétricos; mais precisamente, $x \in \mathbb{Z}$ é representável se e só se $g(a, b) - x$ não é representável.

Em particular, exactamente metade dos inteiros $0 \leq x \leq g(a, b)$ é representável ($g(a, b)$ é sempre ímpar; porquê?)

Não se conhece uma fórmula geral análoga para $n > 2$ (mesmo para $n = 3!$), mas existem vários resultados e algoritmos relacionados com esse problema. Os exercícios seguintes ilustram apenas uma pequena parte desses resultados

6. Mostrar que dados $0 < a < b < c$, com $\text{mdc}(a, b, c) = 1$, o problema de Frobenius está bem posto, ou seja, existe de facto um natural $g(a, b, c)$ tal que todo o $x > g(a, b, c)$ é representável.

Sugestão: sendo $d = \text{mdc}(a, b)$, aplicar a fórmula de Sylvester ao par dm, c para um natural m adequado.

7. Generalizar o argumento do problema anterior para $0 < a_1 < a_2 < \dots < a_n$, com $n > 3$.

Dizemos que um inteiro x é **positivamente representável** por $\{a_1, a_2, \dots, a_n\}$ se existirem inteiros *positivos* u_1, u_2, \dots, u_n tais que

$$x = u_1 a_1 + u_2 a_2 + \dots + u_n a_n.$$

Definimos então $f(a_1, \dots, a_n)$ como o maior inteiro que *não* é positivamente representável por $\{a_1, a_2, \dots, a_n\}$.

8. Mostrar que $f(a_1, \dots, a_n) = g(a_1, \dots, a_n) + \sum_{k=1}^n a_k$; em particular $f(a, b) = ab$.

9. Para cada $0 \leq t < a_1$, definimos m_t como o menor inteiro representável por $\{a_1, a_2, \dots, a_n\}$ e congruente com t módulo a_1 . Mostrar que

- a) Se $x \equiv t \pmod{a_1}$ então x é representável se e só se $x \geq m_t$;
- b) m_t é representável por $\{a_2, \dots, a_n\}$;
- c) $g(a_1, \dots, a_n) = \max\{m_t - a_1 : 0 \leq t < a_1\}$.

10. Seja $d = \text{mdc}(a_2, \dots, a_n)$. Definimos, para cada $0 \leq t < a_1$, m_t tal como no exercício anterior, e, de modo semelhante, r_t como o menor inteiro representável por $\{a_1, \frac{a_2}{d}, \dots, \frac{a_n}{d}\}$ e congruente com t módulo a_1 .

- a) Mostrar que $\{m_t : 0 \leq t < a_1\} = \{dr_t : 0 \leq t < a_1\}$.
- b) Usar o exercício anterior para mostrar que

$$g(a_1, a_2, \dots, a_n) = d g\left(a_1, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right) + a_1(d - 1).$$

- c) Concluir que (ver exercício **8**) $f(a_1, a_2, \dots, a_n) = d f\left(a_1, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right)$.
- d) Calcular $g(6, 10, 15)$.

11. Dados os inteiros a_1, a_2, \dots, a_n , definimos para todo o $1 \leq k \leq n$

$$d_k = \text{mdc}(a_1, a_2, \dots, a_k)$$

e

$$T(a_1, a_2, \dots, a_n) = \sum_{j=2}^n a_j \frac{d_{j-1}}{d_j}.$$

Note-se que T depende da ordem dos a_i .

a) Verificar que se

$$m \equiv 0 \pmod{d_2} \text{ e } m > \frac{a_1 a_2}{d_2}$$

então m é positivamente representável por a_1, a_2 .

b) Mostrar, por indução que para todo o $2 \leq k \leq n$, se

$$m \equiv 0 \pmod{d_k} \text{ e } m > \sum_{j=2}^k a_j \frac{d_{j-1}}{d_j}$$

então m é positivamente representável por a_1, a_2, \dots, a_k .

O caso $k = 2$ foi provado na alínea anterior; suponhamos que $k > 2$ e que a afirmação é verdadeira para $k - 1$;

i) Dado m nas condições indicadas, justificar que

$$m = \sum_{j=2}^{k-1} a_j \frac{d_{j-1}}{d_j} + b d_k \text{ com } b \geq 1;$$

ii) mostrar que a equação

$$a_k x \equiv b d_k \pmod{d_{k-1}}$$

tem uma solução, que designamos x_k satisfazendo $0 < x_k \leq \frac{d_{k-1}}{d_k}$;

iii) mostrar que, por hipótese de indução, existem inteiros positivos x_i , para $1 \leq i < k$, tais que

$$m - x_k a_k = \sum_{i=1}^{k-1} x_i a_i$$

o que completa o passo de indução.

O exercício anterior dá-nos $f(a_1, a_2, \dots, a_n) \leq T(a_1, a_2, \dots, a_n)$.