Teoria Aditiva dos Números

Prof. Carlos Yuzo Shine

A *teoria aditiva dos números* se foca na operação de adição. Apesar de ser a operação mais simples, ela não se mistura muito com o que muitos consideram a operação mais importante da teoria dos números, que é a multiplicação.

Primeiro, um pouco de notação: sendo A e B conjuntos de números, definimos

$$A + B = \{a + b; a \in A \text{ e } b \in B\}$$
$$A - B = \{a - b; a \in A \text{ e } b \in B\}$$

Agora pense nos problemas:

1. Se $|A| = n$ então $|A + A| \geq 2n - 1$, com igualdade se, e somente se, A consiste em n termos consecutivos de uma progressão aritmética.

2. Dizemos que um conjunto A é *livre de somas* quando $(A + A) \cap A = \emptyset$. Em outras palavras, não existem $x, y, z \in A$ tais que $x + y = z$. Por exemplo, o conjunto dos ímpares é livre de somas, e o último teorema de Fermat nos diz que o conjunto das potências n-ésimas, $n \geq 3$, é livre de somas.

   Prove que todo subconjunto com mais de $\lceil n/2 \rceil$ elementos de $[n] = \{1, 2, \ldots, n\}$ não é livre de somas.

3. Todo conjunto finito B tem um subconjunto livre de somas com pelo menos $|B|/3$ elementos.

4. Prove o *teorema de Cauchy-Davenport*: sejam A e B dois subconjuntos não vazios de $\mathbb{Z}/(p)$. Então
   $$|A + B| \geq \min(|A| + |B| - 1, p).$$

5. (O problema de Waring) Seja k um inteiro positivo e
   $$A_k = \{n^k, n \in \mathbb{Z}_+\}$$
   as potências k-ésimas. Definindo
   $$tA_k = \underbrace{A_k + A_k + \cdots + A_k}_{t \text{ vezes}},$$
   qual é o menor valor de t, se existir, para o qual $tA_k = \mathbb{Z}_+$?

   Foi provado na década de 1950 que

   Teorema 1. *Seja $g(k)$ o menor t tal que $tA_k = \mathbb{Z}_+$. Então*

   - $g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$ *se* $2^k \left\{ \left(\frac{3}{2}\right)^k \right\} + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor \leq 2^k$;

- $g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor - 2$ *se* $2^k \left\{ \left(\frac{3}{2}\right)^k \right\} + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor > 2^k$ *e* $\left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor = 2^k$*;*
- $g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor - 3$ *se* $2^k \left\{ \left(\frac{3}{2}\right)^k \right\} + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor > 2^k$ *e* $\left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor > 2^k$.

Prove que $g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$. Na verdade, conjectura-se que $2^k \left\{ \left(\frac{3}{2}\right)^k \right\} + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor \leq 2^k$ para todo k, mas ainda não se provou isso!

6. Prove que, sendo A e B subconjuntos finitos de inteiros, $|A + B| \geq |A| + |B| - 1$.

7. (Ibero) Encontrar o menor número natural n com a seguinte propriedade: entre quaisquer n números distintos do conjunto $\{1, 2, \ldots, 999\}$ pode-se escolher quatro números diferentes a, b, c, d tais que $a + 2b + 3c = d$.

8. (Banco RMM) Sejam U, V, W subconjuntos finitos e não vazios de $\mathbb{Z}$. Prove que

$$|V - W| \leq \frac{|U + V| \cdot |U + W|}{|U|}$$

9. Sejam $n+1$ inteiros $0 = a_0 < a_1 < \ldots < a_n = 2n-1$. Encontre a menor cardinalidade que o conjunto $\{a_i + a_j : 0 \leq i \leq j \leq n\}$ pode ter.

10. (OBM) Dizemos que um conjunto $A \subset \mathbb{N}$ satisfaz a propriedade $P(n)$ se A tem n elementos e $A + A = \{x + y \text{ tal que } x \in A \text{ e } y \in A\}$ tem $\frac{n(n+1)}{2}$ elementos. Dado $A \subset \mathbb{N}$ finito definimos diâmetro de A como sendo a diferença entre o maior e o menor elemento de A. Seja $f(n)$ o menor diâmetro que o conjunto A satisfazendo $P(n)$ pode ter. Mostre que $\frac{n^2}{4} \leq f(n) < n^3$ para todo $n \geq 2$.

    (Se o seu tempo de prova não estiver esgotado, tente melhorar esta estimativa. Por exemplo, tente mostrar que $f(p) < 2p^2$, para todo número primo p.)

11. (Romênia TST) Sejam X e Y subconjuntos finitos de $[0, 1)$ tais que $0 \in X \cap Y$ e $x + y \neq 1$ para todos $x \in X$ e $y \in Y$. Prove que o conjunto $\{x + y - \lfloor x + y \rfloor : x \in X \text{ e } y \in Y\}$ tem pelo menos $|X| + |Y| - 1$ elementos.

12. Seja $p > 3$ primo. O conjunto $\{1, 2, 3, \ldots, p-1\}$ é particionado em três subconjuntos não vazios A, B, C. Prove que existem três números x, y, z, um de cada subconjunto, tais que p divide $x + y - z$.

13. (IMO) Seja A um subconjunto do conjunto $S = \{1, 2, \ldots, 1000000\}$ com exatamente 101 elementos. Demonstre que existem números $t_1, t_2, \ldots, t_{100}$ em S tais que os conjuntos

$$A_j = \{x + t_j \mid x \in A\}, \qquad \text{para} \qquad j = 1, 2, \ldots, 100$$

    são disjuntos dois a dois.

14. (IMO) Sejam $a_1, a_2, \ldots, a_n$ inteiros positivos distintos e M um conjunto de $n-1$ inteiros positivos que não contém o número $s = a_1 + a_2 + \cdots + a_n$. Um gafanhoto pretende saltar ao longo da reta real. Ele começa no ponto 0 e dá n saltos para a direita de comprimentos $a_1, a_2, \ldots, a_n$, em alguma ordem.

    Prove que essa ordem pode ser escolhida de modo que o gafanhoto nunca caia num ponto de M.

15. (Banco da IMO) Seja A um conjunto de n resíduos módulo n^2. Prove que existe um conjunto B de n resíduos módulo n^2 tal que pelo menos metade dos resíduos módulo n^2 pode ser escrito como $a + b$ com $a \in A$ e $b \in B$.

16. (Miklos-Schweitzer) Prove que existem constantes c e n_0 com a seguinte propriedade: se A é um conjunto finito de inteiros, $|A| = n > n_0$, então

$$|A - A| - |A + A| \leq n^2 - cn^{8/5}.$$