Programa Olímpico de Treinamento

Curso de Combinatória – Nível 3

Prof. Carlos Shine

Aula 19

Teoria Aditiva dos Números

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

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

Estimando $|A + A|$

Se $A = \{2^{i-1}, 1 \leq i \leq n\}$, pela unicidade da base 2, temos $|A + A| = \binom{n}{2} + n$, e isso é o melhor que conseguimos. E quanto ao limitante inferior? De fato, temos $2|A| - 1 \leq |A + A| \leq \frac{|A|(|A|+1)}{2}$.

Teorema 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.*

Demonstração: Sejam $a_1 < a_2 < \ldots < a_n$ os elementos de A. Note que

$$a_1 + a_1 < a_1 + a_2 < \ldots < a_1 + a_n < a_2 + a_n < a_3 + a_n < \ldots < a_n + a_n,$$

de modo que $A + A$ tem pelo menos $2n - 1$ elementos.

Para provar o caso de igualdade, note que, para $2 \leq i \leq n - 1$,

$$a_1 + a_1 < a_1 + a_2 < \ldots < a_1 + a_i < a_2 + a_i < \ldots < a_n + a_i < a_n + a_{i+1} < \ldots < a_n + a_n$$

são $2n - 1$ somas distintas, logo no caso de igualdade os termos devem coincidir. Em particular,

$$a_1 + a_{i+1} = a_2 + a_i \iff a_{i+1} - a_i = a_2 - a_1,$$

o que quer dizer que a diferença entre dois termos consecutivos do conjunto A é constante. □

Conjuntos livres de somas

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.

Se fixarmos o conjunto $[n] = \{1, 2, \ldots, n\}$, com os ímpares conseguimos um subconjunto livre de somas com $\lceil n/2 \rceil$ elementos. Será que conseguimos melhor? A resposta é: não.

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

Demonstração: Seja A um subconjunto de $[n]$ com mais de $\lceil n/2 \rceil$. Como é difícil controlar $A + A$, pois vários de seus elementos podem ser maiores do que n, considere no seu lugar o conjunto $X = (A - A) \cap \mathbb{Z}_+^*$, de modo que queremos provar que $X \cap A \neq \emptyset$. Sendo $A = \{a_1, a_2, \ldots, a_k\}$, com $a_1 < a_2 < \ldots < a_k$, note que $0 < a_2 - a_1 < a_3 - a_1 < \ldots < a_k - a_1$, de modo que $|X| \geq |A| - 1$. Mas isso quer dizer que $|A \cap X| = |A| + |X| - |A \cup X| \geq 2|A| - 1 - n > 0$, e acabou. □

A seguir, um resultado que já foi explorado, mas que vale a pena ser repetido.

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

Demonstração: A grande ideia é jogar algo sem muito estrutura (como nosso conjunto B) para algo mais estruturado, no caso o conjunto $\mathbb{Z}/(p)$, p primo grande. Se $p = 3k + 2$, o conjunto $C = \{k + 1, k + 2, \ldots, 2k + 1\} \subset \mathbb{Z}^*/(p)$ é livre de somas e tem $k + 1$ elementos, uma fração $\frac{k+1}{2k+1} > \frac{1}{3}$.

Quando comparamos duas estruturas, a ideia que vem é tentar cruzá-las, com contagem dupla, por exemplo. $\mathbb{Z}^*/(p)$ tem boa estrutura, e a contagem ajuda a encontrar alguém, mesmo que não haja estrutura em B. O que usamos? O "gira-gira". Multiplique todos os elementos de B por x, $1 \leq x < p$, e reduza módulo p. Nenhum $b \in B$ é 0 módulo p, então aparecem todos os resíduos módulo p em $b\mathbb{Z}^*/(p)$, ou seja, C aparece em todo $b\mathbb{Z}^*/(p)$. Mas, definindo $D_x = xB \pmod p$, sendo $|C| > \frac{1}{3}|\mathbb{Z}^*/(p)|$, a probabilidade de algum elemendo de D pertencer a C é maior do que $\frac{1}{3}$, e portanto o valor esperado de elementos de D_x em C é maior do que $|B|/3$. Então existe um D_t com mais de $|B|/3$ elementos de C, e esse é o subconjunto A que queremos. De fato, se $a_1, a_2, a_3 \in A$ são tais que $a_1 + a_2 = a_3$ então $ta_1 + ta_2 \equiv ta_3 \pmod p$, com $ta_1, ta_2, ta_3 \in C$, absurdo. Logo A é livre de somas. □

Teorema de Cauchy-Davenport

E quanto a $\mathbb{Z}/(p)$, o conjunto dos números tomados módulo p primo? O seguinte teorema nos dá uma ideia:

Teorema 4 (Cauchy-Davenport)**.** *Sejam A e B dois subconjuntos não vazios de $\mathbb{Z}/(p)$. Então*

$$|A + B| \geq \min(|A| + |B| - 1, p).$$

Demonstração: Vamos cuidar da parte mais fácil primeiro: se $|A|+|B|-1 \geq p$, $|A|+|B|$ é maior do que p, e pelo princípio da casa dos pombos, os conjuntos $\{x\} - A$ (uma translação de $-A$) e B se interceptam para todo x. Então existem $a \in A$ e $b \in B$ tais que $x - a \equiv b \pmod{p} \iff x \equiv a + b \pmod{p}$, ou seja, $A + B = \mathbb{Z}/(p)$.

A partir de agora, vamos supor que $|A|+|B|-1 < p$. Suponha, por absurdo, que existem conjuntos A e B tais que $A + B \neq \mathbb{Z}/(p)$ e $|A + B| \leq |A| + |B| - 2$. Essa propriedade continua verdadeira se trocamos B por $B - \{b\}$, $b \in B$ (só subtraímos todas as somas em b), de modo que podemos supor sem perda de generalidade que $0 \in B$. Escolha A e B de modo que $|B|$ é minimal. Note que $|B| \geq 2$, pois se $|B| = 1$, bom... $B = \{0\}$.

Agora, vamos definir a *transformada de Davenport*. Temos $A+B \subset A+2B = (A+B)+B$, pois $0 \in B$. Além disso, se $A + B = A + 2B$, $A + 3B = (A + 2B) + B = (A + B) + B = A+2B = A+B$, e indutivamente $A+nB = A+B$. Mas se $a \in A$ e $0 \neq b \in B$, $a+nb \in A+B$ para todo n; só que $a + nb$ cobre todo $\mathbb{Z}/(p)$, e então $A + B = \mathbb{Z}/(p)$, o que não é verdade. Logo $A + B$ está propriamente contido em $A + 2B$, e o conjunto $X = (A + 2B) \setminus (A + B)$ não é vazio.

Sendo $x \in X$, seja

$$B_x^* = \{b \in B \mid x - b \in A + B\}, \quad B_x = B \setminus B_x^*.$$

Note que B_x^* são os caras de B que fazem com que x pertença a $(A + 2B) \setminus (A + B)$, e B_x são... os outros caras. O conjunto B_x é a *transformada de Davenport*.

Agora, veja que $0 \notin B_x^* \neq \emptyset$ e $0 \in B_x \subset B$. Agora, é claro que $A + B_x \subset A + B$ e $\{x\} - B_x^* \subset A + B$, de modo que

$$(A + B_x) \cup (\{x\} - B_x^*) \subset A + B.$$

Finalmente, note que se $(A+B_x)\cap(\{x\}-B_x^*) \neq \emptyset$, ocorre $a+b_x = x-b_x^* \iff a+b_x^* = x - b_x \in A + B$ e $b_x \in B_x^*$, o que é absurdo pois $B_x^* \cap B_x = \emptyset$. Enfim,

$$|A + B| \geq |A + B_x| + |\{x\} - B_x^*| = |A + B_x| + |B_x^*| = |A + B_x| + |B| - |B_x|$$

Assim, o problema acabou: de fato, se trocarmos A e B por A e B_x, temos $1 \leq |B_x| < |B|$, $|A + B_x| < |A + B| < p$ e

$$|A + B_x| \leq |A + B| - |B| + |B_x| \leq |A| + |B| - 2 - |B| + |B_x| = |A| + |B_x| - 2,$$

ou seja, conseguimos um exemplo com $|B_x| < |B|$ menor ainda, o que é absurdo. □

A igualdade ocorre em uma das seguintes situações:

- $|A| + |B| > p$;
- $|A| = 1$ ou $|B| = 1$;
- $B = \{c\} - \overline{A}$ para algum $c \in \mathbb{Z}/(p)$;
- A e B são progressões aritméticas com mesma razão.

A demonstração está em [2].

Problemas

1. (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 5. *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!

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

3. (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 $a + 2b + 3c = d$.

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

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

5. 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.

6. (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.)

7. (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.

8. 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 $x+y-z$.

9. (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.

10. (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.

11. (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 $b \in B$.

12. (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
$$|A-A| - |A+A| \leq n^2 - cn^{8/5}.$$

Bibliografia

1. T. Tao, *Lecture Notes 1 for 254A*. Disponível em
   `http://www.math.cmu.edu/~af1p/Teaching/AdditiveCombinatorics/Tao.pdf`
2. Ø. J. Rødseth, *Sumsets* mod p. Disponível em
   `http://www.folk.uib.no/nmaoy/papers/sumsetsR.pdf`
3. N. Alon, J. H. Spencer, P. Erdős, *The Probabilistic Method*, John Wiley & Sons 1992.

Respostas, Dicas e Soluções

1. É só considerar $2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1$, que é menor do que 3^k: como as únicas potências k-ésimas menores que 3^k são 2^k e 1, devemos usar a maior quantidade possível de 2^ks, que é $\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1$, e cobrir o resto, que é $2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 - \left(\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 \right) 2^k = 2^k - 1$, com 1s. Com isso, precisamos de pelo menos $\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 + 2^k - 1 = \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + 2^k - 2$ potências.

2. Translade A e B de modo que $\max A = \min B = 0$. Note que A só tem números não positivos e B só tem números não negativos, e que $A \cup B \subset A + B$, pois $0 \in A$ e $0 \in B$. Logo $|A + B| \geq |A \cup B| = |A| + |B| - 1$.

3. A resposta é $n = 835$. Para ver isso, considere o exemplo com os 834 números de 166 a 999. O menor valor de $a + 2b + 3c$ é $168 + 2 \cdot 167 + 3 \cdot 166 = 1000$.

   Agora, considere 835 números entre os mais de 834 escolhidos, e sejam eles $m = a_1 < a_2 < \ldots < a_{835} = M$. Temos $M \geq m + 834$, de modo que $-3m \geq 3 \cdot 834 - 3M$, e $M - 3m \geq 3 \cdot 834 - 2M \geq 3 \cdot 834 - 3 \cdot 999 = 504$. A ideia é comparar $M - 3m$ com $a_i + 2a_j$, $1 < i, j < 835$. Fixe $k = M - 3m$ e considere a equação $x + 2y = k$. Há pelo menos $k/3 - 1 \geq 167$ soluções disjuntas para essa equação: $(k - 2i, i)$, $1 \leq i \leq 167$ (note que sempre temos $x > y$, então não há perigo de ocorrer repetições). Então para que não ocorra $a + 2b = M - 3m$ devemos ter $b = m$ ou um dos números a, b não está entre os escolhidos. Isso elimina pelo menos $167 - 1 = 166$ números, sobrando no máximo $999 - 166 = 833$, e aí obtemos uma contradição, de modo que existem a, b com $a + 2b = M - 3m$.

4. Reescreva a desigualdade como $|V - W| \cdot |U| \leq |U + V| \cdot |U + W|$ e considere o produto cartesiano $(U + V) \times (U + W)$. Note que ele contém os pares $(u + v, u + w)$, $u \in U$, $v \in V$ e $w \in W$. Note que $(u_1 + v_1, u_1 + w_1) = (u_2 + v_2, u_2 + w_2) \iff v_1 - v_2 = w_1 - w_2 = u_2 - u_1 \implies v_1 - w_1 = v_2 - w_2$. Assim, dado $u \in U$ e $x \in V - W$, conseguimos, escolhendo um par (v, w) adequado para cada x, pelo menos um elemento $(u + w + x, u + w)$ de $(U + V) \times (U + W)$, e não temos repetições (só escolhemos um representante para cada $u - v$). Logo

$$\begin{aligned} |U + V| \cdot |U + W| &= |(U + V) \times (U + W)| \\ &\geq |\{(u + v, u + w) : u \in U, v \in V, w \in W\}| \\ &\geq |U| \cdot |V - W|. \end{aligned}$$

5. A resposta é $3n$, obtida para $a_i = i$ para $0 \leq i < n$: as somas são $0, 1, \ldots, 3n - 1$. Vamos provar que pelo menos $3n$ somas aparecem em qualquer situação. Primeiro, seja $A = \{a_i : 0 \leq i \leq n\}$; note que $(A + \{2n-1\}) \cup (A + \{0\})$ já tem $2(n+1) - 1 = 2n + 1$ somas diferentes, pois todo elemento de $A + \{2n - 1\}$ é maior ou igual que os elementos de A, com igualdade só para o $2n - 1$. Faltam $n - 1$ elementos!

   Agora, seja C o conjunto dos $2n - (n + 1) = n - 1$ números entre 0 e $2n - 1$ que não foram escolhidos para compor A. Note que as somas podem ir de 0 a $2(2n - 1)$, então consideremos também $C + \{2n - 1\}$. Provaremos que, para $c \in C$, pelo menos um dos dois números c ou $c + 2n - 1$ está em $A + A$. Como $|C| = n - 1$, isso termina o problema.

   Para isso, seja t o inteiro tal que $a_{t-1} < c < a_t$ e pensemos em $c + 2n - 1$. Não há chance para que $a_i + a_j = c + 2n - 1$ se um dos índices é menor do que t, então considere os conjuntos $X = \{a_t, a_{t+1}, \ldots, a_n = 2n - 1, a_1 + 2n - 1, a_2 + 2n - 1, \ldots, a_{t-1} + 2n - 1\}$ e $Y = \{c + 2n - 1 - a_i : 1 \leq i \leq n - 1\}$. Temos $|X| = n$ e $|Y| = n - 1$ e todos

os elementos de $X \cup Y$ maiores do que c e menores do que $c + 2n - 1$, num total de no máximo $2n - 2$ números. Logo $X \cap Y \neq \emptyset$. Assim, existem i e j tais que $a_i = c + 2n - 1 - a_j \iff a_i + a_j = c + 2n - 1$, ou seja, $c + 2n - 1 \in A + A$ ou $a_i + 2n - 1 = c + 2n - 1 - a_j \iff a_i + a_j = c$, ou seja, $c \in A + A$, e o problema acabou.

6. Dado um conjunto finito $A \subset \mathbb{N}$, denotaremos por $d(A)$ o diâmetro de A. Temos duas desigualdades a provar:

   (i) $f(n) \geq \frac{n^2}{4}$, para todo $n \geq 2$.
   Considere um conjunto $A = \{a_1, a_2, \ldots, a_n\}$, $a_1 < a_2 < \cdots < a_n$, $n \geq 2$ que satisfaz $P(n)$. Assim, $A+A = \{a_1+a_1, a_1+a_2, \ldots, a_n+a_n\}$ tem $\frac{n(n+1)}{2}$ elementos. Como $a_1 + a_1 < a_1 + a_2 < \cdots < a_n + a_n$, temos que $(a_n + a_n) - (a_1 + a_1) + 1 \geq \frac{n(n+1)}{2} \implies a_n - a_1 \geq \frac{n^2}{4} + \frac{n-2}{4} \geq \frac{n^2}{4} \implies d(A) \geq \frac{n^2}{4}$. Isto demonstra (i).

   (ii) $f(n) < n^3$, para todo $n \geq 2$.
   Vamos fazer isso por indução. Como $\{0, 1\}$ satisfaz $P(2)$, temos que $f(2) \leq 1 < 2^3$. Agora, vamos supor que $f(n) < n^3$ para algum $n \geq 2$. Seja $A_n = \{a_1, a_2, \ldots, a_n\} \subset \mathbb{N}$ tal que A_n satisfaz $P(n)$ e $d(A_n) = f(n) < n^3$. Sem perda de generalidade, podemos supor que $0 = a_1 < a_2 < \cdots < a_n = d(A_n)$, bastando para isto subtrair de cada elemento de A_n o menor de seus elementos.
   Agora, queremos achar $a_{n+1} \in \mathbb{N} - A_n$ tal que $A_{n+1} = \{a_1, a_2, \ldots, a_{n+1}\}$ satisfaça $P(n+1)$ e $d(A_{n+1}) < (n+1)^3$. Como $A_n + A_n$ tem $\frac{n(n+1)}{2}$ elementos e $A_{n+1} + A_{n+1} = (A_n + A_n) \cup \{a_i + a_{n+1} \mid 1 \leq i \leq n+1\}$, temos que $a_{n+1} \in \mathbb{N} \setminus A_n$ e A_{n+1} satisfaz $P(n+1)$ se, e somente se, $a_{n+1} + a_k \neq a_i + a_j \in A_n + A_n$ ou $a_{n+1} + a_{n_1} \neq a_i + a_j \iff a_{n+1} \neq \frac{a_i+a_j}{2}$, ou seja, $a_{n+1} \notin P = \{a_i + a_j - a_k \mid 1 \leq i, j, k \leq n\} \cup \left\{\frac{a_i+a_j}{2} \mid 1 \leq i, j \leq n\right\}$. Como $|P| \leq n^3 + \frac{n(n+1)}{2}$ (no máximo n^3 escolhas para $a_i + a_j - a_k$ e no máximo $\binom{n}{2} + n$ escolhas para $\frac{a_i+a_j}{2}$), temos que $a_{n+1} \leq n^3 + \frac{n(n+1)}{2}$, pois basta escolher a_{n+1} como o menor natural que não está em P. Assim, $f(n+1) \leq d(A_{n+1}) < (n+1)^3$. Por indução finita em n, temos que (ii) é verdade, o que completa nossa demonstração.
   Vamos ainda, verificar que, para P primo, $f(p) < 2p^2$. Para isto, construímos o conjunto $A = \{k + 2pg(k), 0 \leq k \leq p-1\}$, onde $g(k) = k^2 \bmod p$ é o resto da divisão de k^2 por p. temos $d(A) \leq p - 1 + 2p(p-1) = 2p^2 - p - 1 < 2p^2$ e se tivéssemos $i + 2pg(i) + j + 2pg(j) = r + 2pg(r) + s + 2pg(s) \iff i + j - (r+s) = 2p(g(i) + g(j) - (g(r) + g(s)))$, então como $-2p < i + j - (r+s) < 2p$ é múltiplo de $2p$

$$\begin{aligned} & i + j + 2p(g(i) + g(j)) = r + s + 2p(g(r) + g(s)) \\ \iff & i + j = r + s \text{ e } g(i) + g(j) = g(r) + g(s). \end{aligned}$$

   Note que o $2p$ multiplicando $g(k)$ não foi ao acaso. A ideia era exatamente se aproveitar do fato de que $-2p < i + j - (r+s) < 2p$.

Assim, $i - r = s - j$ e $i^2 + j^2 \equiv r^2 + s^2 \pmod p$, logo

$$\begin{aligned} &(i-r)(i+r) \equiv (s-j)(s+j) \pmod p \\ \iff &i - r \equiv s - j \equiv 0 \pmod p \text{ ou } i + r \equiv s + j \pmod p. \end{aligned}$$

Portanto $i = r$ e $s = j$ ou $i = s$ e $r = j$.

Novamente, $k^2 \bmod p$ não foi escolhido ao acaso: usamos o fato de que $i - r = s - j$ e a fatoração da diferença de quadrados.

7. Imite a demonstração do teorema de Cauchy-Davenport. É praticamente igual! Defina $X + Y$ módulo 1, e para provar que $X + Y \neq X + 2Y$, leve em consideração que $ny \in X + Y$ para todo n inteiro positivo e, portanto, ny nunca é inteiro; ou seja, $nY \subset X + Y$ é infinito, absurdo.

8. Suponha por absurdo que exista uma partição sem a propriedade do enunciado. Podemos supor, sem perda de generalidade, que A é um conjunto com menos elementos, e também podemos supor que $1 \in A$, pois basta multiplicar todos os números por a^{-1}, para algum $a \in A$. Seja k o número tal que $1, 2, \ldots, k \in A$ e $k + 1 \in B$. Seja $c \in C$, i com $1 \leq i \leq k$. Se $c \pm i \in B$, $(i, c \pm i, c) \in A \times B \times C$, então $c \pm i \notin B$. Se $c + i \in C$ e $c - (k + 1 - i) \in A$, $(c - k - 1 + i, k + 1, c + i) \in A \times B \times C$ também.

   Seja $c_1 = \min C$. Então $c_1 - (k + 1 - i) \in A$ e, portanto, $c_1 + i \in A$, ou seja, A contém $\{1, 2, \ldots, k\} \cup \{c_1 - 1, c_1 - 2, \ldots, c_1 - k\} \cup \{c_1 + 1, c_1 + 2, \ldots, c_1 + k\}$. Essa ideia também vale se tomarmos o próximo elemento de C, e assim por diante. Logo temos $|A| > |C|$, o que é uma contradição, e o problema acabou.

9. Vamos supor, sem perda de generalidade, $1 = t_1 < t_2 < \ldots < t_{100}$. Quando dois conjuntos A_i e A_j têm interseção? Quando $x_i + t_i = x_j + t_j \iff t_j = x_i - x_j + t_i$. Ou seja, devemos nos preocupar com $A - A$.

   Agora, vamos construir um exemplo indutivamente. Já escolhemos $t_1 = 1$. Suponha que já escolhemos $t_1, \ldots, t_k$. Para escolher t_{k+1}, cada valor de t_i, $1 \leq i \leq k$, proíbe $\binom{101}{2} = \frac{101 \cdot 100}{2}$ números (as escolhas de $x_i > x_j$) além, é claro, dos k valores anteriores. Então há $k \cdot 101 \cdot 50 + k \leq 99 \cdot (50 \cdot 101 + 1) < 1000000$ números proibidos, e sempre sobra pelo menos um para escolher.

10. Indução sobre n. Não há o que se provar para $n = 1$ e o problema é imediato se $n = 2$. Suponha então que $n > 1$, e seja a_n o maior dos números a_i e $m = \max M$. Caso $s - a_n \in M$ e $m > s - a_n$ (ou seja, $s - a_n$ não é o máximo), então para algum i, $1 \leq i \leq n - 1$, $s - a_i$ e $s - a_i - a_n$ estão ambos fora de M: são $n - 1$ pares $(s - a_i, s - a_i - a_n)$, nenhum desses números é igual a $s - a_n$, que é um elemento de M, e sobram $n - 2$ outros elementos em M. Aí, aplicamos a hipótese de indução para os $n - 2$ números tirando a_i e a_n e os $n - 3$ elementos de M tirando m e $s - a_n$, que são ambos maiores do que $s - a_i - a_n$, e terminamos pulando em $s - a_i$ e s.

    No outro caso, aplicamos a hipótese de indução para os a_i's tirando a_n e $M \setminus \{m\}$. Note que agora ou $s - a_n \notin M$ ou $s - a_n = m$, então podemos fazer isso. Fazemos

então os $n-1$ pulos pela hipótese de indução e colocamos m de volta. Se m não está em nenhum dos pulos, basta dar o último pulo de tamanho a_n e terminamos; se m está no k-ésimo pulo (note que m é o último lugar em que isso pode acontecer), trocamos o k-ésimo pulo por a_n, ultrapassamos m e depois usamos os outros pulos. Com isso, o passo de indução está completo.

11. Escolha um conjunto B com n elementos aleatórios de $\mathbb{Z}/(n^2)$, com reposição. Calculemos a probabilidade de um resto fixado r não pertencer a $A+B$: basta que nenhum dos números $r-a$, $a \in A$, pertença a B. Isso ocorre com probabilidade $\left(1-\frac{1}{n}\right)^n$ (a chance de não sortearmos um elemento da forma $r-a$ é $1-\frac{1}{n}$).

    Como $n^n > 2(n-1)^n \iff \left(1-\frac{1}{n}\right)^n < \frac{1}{2}$ para $n \geq 2$, temos que a probabilidade de r não pertencer a $A+B$ é menor do que $\frac{1}{2}$, e o valor esperado de números que não estão em $A+B$ é menor do que $n^2/2$. Logo o valor esperado de números que estão em $A+B$ é maior do que $n^2/2$ e existe um B desejado. De fato, para n grande existe um conjunto B tal que $A+B$ tem pelo menos $n^2\left(1-\frac{1}{e}\right)$ elementos!

12. Considere o seguinte lema:

    Lema 1. *Suponha que uma diferença c de $A-A$ possa ser escrita de k maneiras na forma $a_i - a_j$, $a_i, a_j \in A$. Então existe um conjunto $V \subset A$ com pelo menos $k/3$ elementos tal que cada diferença $v_i - v_j$ de $V-V$ também apareça em $(A \setminus V)-(A \setminus V)$.*

    Para provar esse lema, note que as k diferenças formam várias progressões aritméticas disjuntas; escolha para V os termos de ordem par das PAs (ou seja, se a PA é $a, a+r, a+2r$ escolhemos $a+r$), e temos pelo menos $k/3$ elementos. Para ver por que dá certo, basta deslocar um termo de cada termo da diferença na PA correspondente.

    Aí temos

$$\begin{aligned}|A-A| - |A+A| \leq |A-A| &\leq |(A \setminus V) - (A \setminus V)| + |(A \setminus V) - V| + |V - (A \setminus V)| \\ &\leq 2|V|(n-|V|) + (n-|V|)^2 = n^2 - |V|^2 \leq n^2 - (k/3)^2,\end{aligned}$$

    o que resolve o problema se $k \geq C \cdot n^{4/5}$, ou seja, alguma diferença aparece mais do que $C \cdot n^{4/5}$ vezes.

    Caso contrário, seja $s = |A+A|$ e $t = |A-A|$. Suponha que cada soma s_i, $1 \leq i \leq s$, seja escrita na forma $a_i + a_j$ de x_i maneiras e que cada diferença t_i, $1 \leq i \leq t$, seja escrita na forma $a_i - a_j$ de y_i maneiras. Então, como há n^2 pares (a_i, a_j),

$$\sum_{i=1}^{s} x_i = \sum_{i=1}^{t} y_i = n^2$$

    Além disso, como $a_i + a_j = a_p + a_q \iff a_i - a_p = a_q - a_j$, existem x_u^2 quádruplas (a_i, a_j, a_p, a_q) com $a_i + a_j = a_p + a_q = s_u$ e y_v^2 quádruplas (a_i, a_j, a_p, a_q) com $a_i - a_p = a_q + a_j$, temos também

$$\sum_{i=1}^{s} x_i^2 = \sum_{i=1}^{t} y_i^2 = S$$

Como $1 \leq y_i \leq C \cdot n^{4/5}$, S é maximizado quando todos os y_i's são 1 ou $C \cdot n^{4/5}$. Achando a quantidade de 1's e $C \cdot n^{4/5}$'s, temos

$$S \leq \frac{n^2 - t}{Cn^{4/5} - 1} \cdot (Cn^{4/5})^2 + t - \frac{n^2 - t}{Cn^{4/5} - 1} = (n^2 - t)(Cn^{4/5} + 1) + t$$

Por Cauchy-Schwartz, $S \cdot s \geq n^4 \iff s \geq \frac{n^4}{S} \geq \frac{n^4}{(n^2-t)(Cn^{4/5}+1)+t}$.

Então, sendo $x = n^2 - t$,

$$|A - A| - |A + A| \leq n^2 - x - \frac{n^4}{xCn^{4/5} + n^2}$$

Se $x \geq C'n^{8/5}$, o resultado segue imediatamente. Caso contrário, $xCn^{4/5} + n^2 < C'n^{12/5} + n^2 < C''n^{12/5}$ para n suficientemente grande e $\frac{n^4}{xCn^{4/5}+n^2} > C'''n^{8/5}$, e o problema termina de qualquer jeito.