Teorema de Roth

Thiago Landim

Nível U

Sumário

1 Introdução

1.1 História

Nos anos 20, o matemático Baudet fez a seguinte conjectura:

Se dividirmos os naturais em duas classes, alguma delas possui progressões aritméticas de comprimento arbitrário?

Embora para todos a resposta fosse óbvia (e afirmativa!) ninguém era capaz de demonstrar. Logo o problema foi criando fama, e, em 1927, foi resolvido por um jovem matemático holandês que fora estudar em Göttingen chamado Bartel van der Waerden.

Teorema 1 (van der Waerden, versão finitária)
Dados dois inteiros positivos r e k, existe N tal que, se o conjunto $\{1, 2, \ldots, N\}$ é particionado em r classes, existe uma classe que contém uma progressão aritmética de comprimento k.

Como o van der Waerden percebeu, esse resultado é equivalente a um outro de enunciado semelhante.

Teorema 2 (van der Waerden, versão infinitária)
Para toda partição $\mathbb{N} = \bigcup_{i=1}^{r} C_i$, existe algum C_j que contém progressões aritméticas de tamanho arbitrário.

Problema (Argumento de compacidade)**.** Mostre que os dois teoremas acima são equivalentes.
(Dica: Primeiro escolha a cor do 1, depois escolha a cor do 2, depois a cor do 3, e assim por diante...)

O resultado despertou a curiosidade de diversos matemáticos. Erdös e Turán acreditavam que o *real motivo* da veracidade do teorema é que algum C_j será "suficientemente grande". Para reduzir a tinta necessária para imprimir esse material, denote $[N] \coloneqq \{1, 2, \ldots, N\}$. Eles definiram $r(N)$ o tamanho máximo de um conjunto em $[N]$ sem 3-PAs, e provaram que para todo $\varepsilon > 0$, existe $N_0 = N_0(\varepsilon)$ tal que para $N > N_0$ vale

$$r(N) \leq \left(\frac{3}{8} + \varepsilon\right) N.$$

Eles, então, conjecturaram que $r(N) = o(N)$, enquanto Szekeres conjecturou algo ainda mais forte

$$r\left(\frac{1}{2}(3^k + 1)\right) = 2^k,$$

ou seja, que $r(N) = O(N^{\frac{\log 2}{\log 3}})$. Os primeiros desenvolvimentos nessas conjecturas foram cotas inferiores, e mostraram que a conjectura de Szekeres estava incorreta. Mas ainda, para todo $\delta > 0$, $r(N) > N^{1-\delta}$ para todo N suficientemente grande. O exemplo de Behrend, construído em 1946, só veio a ser melhorado 62 anos depois! Por outro lado, as cotas superiores foram mais tardias, apenas em 1953 Klaus Roth demonstrou que a conjectura de Erdös e Turán é verdadeira, e ele deu a cota superior

$$r(N) = O\left(\frac{N}{\log \log N}\right).$$

Seguiu, implicitamente, a seguinte conjectura, a qual o Erdös posteriormente ofereceu \$1000 pela solução. Se $r_l(N)$ é o tamanho máximo de um conjunto em $[N]$ sem l-PAs, então $r_l(N) = o(N)$. Apesar de grandes

esforços, esse resultado não parecia se render. O primeiro avanço após Roth foi feito por Szemerédi, que em 1969 demonstrou que $r_4(N) = o(N)$. Melhorando os seus métodos, ele finalmente conseguiu demonstrar a conjectura final, que hoje recebe o seu nome, usando Teoria dos Grafos. A respeito desse resultado, o Erdös disse: "eu sinto que nunca 1000 dólares foram tão merecidos. De fato, diversos dos meus colegas apontaram que a minha oferta violava a lei do salário mínimo".

Teorema 3 (Teorema de Szemerédi, 1975)
Se $r_l(N)$ é o tamanho máximo de um conjunto em $[N]$ sem l-PAs, então

$$r_l(N) = o(N).$$

Apenas dois anos depois, o Hillel Furstenberg demonstrou o mesmo resultado utilizando métodos da Teoria Ergódica. Com o tempo, foram desenvolvidos outros métodos que poderiam ser usados para demonstrar o Teorema de Szemerédi: T. Gowers utilizou a Análise Harmônica em 2001, e Nagle, Rödl, Schacht, Skokan, e, independentemente, o Gowers, utilizaram o Lema da Regularidade em Hipergrafos, alguns anos depois.

As cotas dadas pelo Lema da Regularidade são quantitativas, mas sem precisão, enquanto que as cotas usando Teoria Ergódica são apenas assintóticas: $r_l(N) = o(N)$. As melhores cotas são dadas por métodos da Análise Harmônica. A cota encontrada pelo Gowers é a melhor atualmente, e é dada por

$$r_l(N) \leq \frac{N}{(\log\log N)^{2^{-2^{l+9}}}}.$$

É possível enunciar o teorema de Roth de maneira mais concisa. Para tanto, vamos começar definindo como medir conjunto!

Definição 4
Seja $A \subseteq \mathbb{N}$ um subconjunto dos naturais. Definimos sua *densidade superior* por

$$\bar{d}(A) = \limsup_{N\to\infty} \frac{|A \cap \{1, 2, \cdots, N\}|}{N}.$$

Se esse limite existir, dizemos simplesmente a densidade de A, e escrevemos $d(A)$.

Obs.: Note que a fração dentro do limite mede a probabilidade de, ao sortearmos aleatoriamente um número de 1 a N, ele estar em A.

Com essa definição, agora podemos enunciar o teorema de maneira mais concisa.

Teorema 5 (Teorema de Roth, 1953)
Se $A \subseteq \mathbb{N}$ um conjunto sem 3-PAs, então $\bar{d}(A) = 0$.

Sabemos que existem PAs de tamanho arbitrário, mas existe alguma progressão aritmética infinita? Por exemplo, o conjunto dos pares tem densidade $\frac{1}{2}$, e é claramente uma PA infinita. Por outro lado, imagine que construímos o conjunto A colocando $n!$ números em A e pulando $(n+1)!$.

2 Cotas Inferiores

2.1 Cota inicial

Para fazer sua conjectura, Szekeres se baseou em uma construção bastante natural e que parece ser ótima. Vamos tentar construir um conjunto livre de 3-PAs com um algoritmo guloso. Começamos com os números inicias e vamos pulando os números que formariam uma 3-PA. Ficaríamos com a sequência conhecida como sequência de Stanley:

$$0 \quad 1 \quad 3 \quad 4 \quad 9 \quad 10 \quad 12 \quad 13 \quad 27 \quad 28 \quad 30 \quad \dots .$$

Essa sequência tem uma propriedade muito interessante: ela é formada pelos números escritos apenas com 0 e 1 na base 3! Assim, concluímos que de 0 a $1 + 3 + 3^2 + \cdots + 3^k = \frac{3^k-1}{2}$ temos 2^k números dessa forma. Se somarmos 1 para que essa sequência comece em 1, nós vamos ter 2^k números de 1 a $\frac{3^k+1}{2}$, de onde vem a conjectura do Szekeres.

Essa sequência tem um problema: a quantidade alta de termos pequenos nos obriga a separar demais os números altos. Assim, embora seja a cota máxima para valores pequenos, ela não é boa assintoticamente.

2.2 Salem & D. Spencer

Em 1942, Salem e Donald Spencer mostraram que a conjectura de Szekeres estava errada. Mais especificamente, eles mostraram que

$$r(N) \geq N^{1-\frac{\log 2+\varepsilon}{\log\log N}}.$$

Não iremos nos preocupar muito com a constante, de modo a simplificar um pouco a solução.

Para fazer isso, eles se basearam na ideia anterior: escrever os números em uma base que não é a decimal. Mas, dessa vez, não teremos base 3. Seja $d > 1$ um inteiro qualquer e n um múltiplo de d (essa condição não é importante, mas facilita a nossa construção). Então vamos considerar o conjunto S dos inteiros da forma

$$m = a_0 + a_1(2d-1) + \cdots + a_{n-1}(2d-1)^{n-1}.$$

tais que entre os dígitos a_i exatamente $\frac{n}{d}$ são 0, exatamente $\frac{n}{d}$ são 1, ..., exatamente $\frac{n}{d}$ são $d-1$. Portanto

$$|S| = \frac{n!}{\left(\frac{n}{d}\right)!^d}.$$

Por outro lado, para todo $m \in S$, $m < (d-1)^n$.

Note agora que S não possui 3-PA. De fato, suponha que m, m' e m'' em S satisfazem $m + m' = 2m''$, e sejam a_i, a_i', a_i'' seus dígitos. Como a_i, a_i', $a_i'' \leq d-1$, então $a_i + a_i' \leq 2d-2$ e $2a_i \leq 2d-2$ (e aqui está o motivo de escolhermos escrever o número na base $2d-1$). Assim, não haverá o famoso "vai um", de onde segue que para todo i

$$a_i + a_i' = a_i''.$$

Se $a_i'' = 0$, então $a_i = a_i' = 0$. De onde segue que m, m' e m'' têm os mesmos dígitos iguais a 0. Analogamente, como nenhum dígito pode mais ser 0, se $a_i'' = 1$, então $a_i = a_i' = 1$. Pode-se, então, demonstrar por indução em k que $a_i = a_i' = a_i'' = k$ para todo $0 \leq k \leq d-1$, logo $m = m' = m''$. Além disso, por Stirling

$$|S| \sim \frac{n^n\sqrt{2\pi n}e^{-n}}{\left(\left(\frac{n}{d}\right)^{n/d}\sqrt{2\pi\frac{n}{d}}e^{n/d}\right)^d} > \left(\frac{d}{Cn}\right)^{d/2} d^n,$$

onde C é uma constante arbitrariamente próxima de 2π.

Para finalizar a prova, escolha uma sequência crescente de inteiros $\omega(d)$ tal que $\lim_{d\to\infty} \frac{\omega(d)}{\log d} = \infty$, $\lim_{d\to\infty} \frac{\log \omega(d)}{\log d} = 0$ e $\omega(d+1) - \omega(d) = O(1)$, por exemplo, $\omega(d) = \lfloor \log^2 d \rfloor$ (se não estivéssemos supondo n múltiplo de d, poderíamos supor aqui $\omega(d+1) - \omega(d) = o(1)$). Dado N qualquer, tome d tal que

$$(2d-1)^{d\omega(d)} \leq N < (2d+1)^{(d+1)\omega(d+1)}.$$

Resta apenas muita conta para encontrarmos o valor. Das desigualdades,

$$\begin{aligned} r(N) &\geq r((2d-1)^{d\omega(d)}) \\ &> \left(\frac{d}{Cd\omega(d)}\right)^{d/2} d^{d\omega(d)}, \end{aligned}$$

de onde segue que

$$\frac{r(N)}{N} > \left(\frac{1}{C\omega(d)}\right)^{d/2} \frac{d^{d\omega(d)}}{(2d+1)^{(d+1)\omega(d+1)}}.$$

Portanto

$$\log\left(\frac{N}{r(N)}\right) < (d+1)\omega(d+1)\log(2d+1) - d\omega(d)\log d + \frac{d}{2}\log\omega(d) + \frac{d}{2}\log C = O(d\log d).$$

Por outro lado, sabemos que

$$\begin{aligned} \log N &\geq d\omega(d)\log(2d-1) \\ \log\log N &< \log(d+1) + \log\omega(d+1) + \log\log(2d+1), \end{aligned}$$

o que nos permite a comparação

$$\frac{\log N}{\log\log N} > d\omega(d)[1+o(1)].$$

Finalmente, concluímos a cota

$$\log\left(\frac{N}{r(N)}\right) = O\left(\frac{\log N}{\log\log N}\right),$$

ou seja

$$r(N) = \frac{N}{e^{O(\log N/\log\log N)}},$$

mostrando que a conjectura de Szekeres era falsa.

Mais ainda, para todo $\delta > 0$, é falso que $r(N) = O(N^{1-\delta})$.

2.3 Behrend

Behrend se baseou na solução de Salem e Spencer, mas usou o fato que a esfera em $\mathbb{R}^n$ é uniformemente convexa. Dessa forma, ele simplificou o resultado e melhorou a cota. Se x, y, z são vetores na esfera tais que $x + y = 2z$, então $|x+y| = |2z| = 2 = |x| + |y|$. Assim, x e y estão no mesmo sentido, de onde segue que $x = y = z$. Obviamente, estamos preocupados apenas com os pontos inteiros, logo para um dado k, nós observaremos o conjunto $S(n,k) = \{a \in \mathbb{Z}^n \mid |a|^2 = k\}$.

Agora retornemos a nossa solução anterior, vamos analisar números da forma

$$m = a_0 + a_1(2d-1) + \cdots + a_{n-1}(2d-1)^{n-1}$$

satisfazendo $0 \leq a_i < d$. A cada um desses números, podemos associar um vetor em $\mathbb{Z}^n$ dado por $a = (a_0, a_1, \ldots, a_{n-1})$. Note que $0 \leq |a|^2 < n(d-1)^2$, portanto cada a está em algum $S(n,k)$ para $0 \leq k < n(d-1)^2$. Como acima, a escolha dos a_i implica que podemos somar números dessa forma termo a termo.

Problema. Mostre que o conjunto $P(n,k)$ dos números m associados a vetores a em $S(n,k)$ é um conjunto livre de 3-PAs.

Assim, como temos d^n números dessa forma, algum dos $P(n,k)$ contém pelo menos

$$\frac{d^n}{n(d-1)^2+1} > \frac{d^{n-2}}{n}$$

números.

Como todos esses números são $< (2d-1)^n$, vemos que $r((2d-1)^n) \geq d^{n-2}/n$. Seja N um número natural. Fixado n a determinar, escolha d tal que

$$(2d-1)^n \leq N < (2d+1)^n.$$

Segue, então, que

$$d > \frac{N^{1/n}-1}{2}$$

e

$$\begin{aligned} r(N) &\geq r((2d-1)^n) \\ &\geq \frac{d^{n-2}}{n} \\ &> \frac{(N^{1/n}-1)^{n-2}}{n2^{n-2}} \\ &= \frac{N^{1-2/n}}{n2^{n-2}}\left(1-\frac{1}{N^{1/n}}\right)^{n-2}. \end{aligned}$$

Desejamos nos preocupar apenas com a fração, que é uma expressão mais simpática. Note que a segunda expressão lembra o limite fundamental da exponencial. Para que esse limite não exploda, devemos ter que

$$\frac{1}{N^{1/n}} \lesssim \frac{1}{n},$$

ou seja, que

$$n \log n \lesssim \log N.$$

Com isso em mente, vamos observar a nossa fração. Podemos escrevê-la como

$$N^{1-\frac{2}{n}-\frac{\log n}{\log N}-\frac{(n-2)\log 2}{\log N}}.$$

Note, então, que o terceiro termo é dominado pelo quarto, logo nós só precisamos nos preocupar com o segundo e o quarto. Pela desigualdade das médias,

$$\frac{2}{n}+\frac{(n-2)\log 2}{\log N} \gtrsim 2\sqrt{\frac{2\log 2}{\log N}},$$

e ocorre a igualdade quando $n \sim \sqrt{\frac{2\log N}{\log 2}}$. Assim, segue que, para qualquer $\varepsilon > 0$ e para N suficientemente grande, existe um conjunto livre de 3-PAs em $[N]$ de tamanho

$$N^{1-\frac{2\sqrt{2\log 2}+\varepsilon}{\sqrt{\log N}}}.$$

Problema. Faça as contas acima com cuidado tomando desde o início $n = \left\lfloor \sqrt{\frac{2\log N}{\log 2}} \right\rfloor$.

Problema. No lugar de fixar n, e escolher d, nós podemos fixar d e escolher n. Suponha

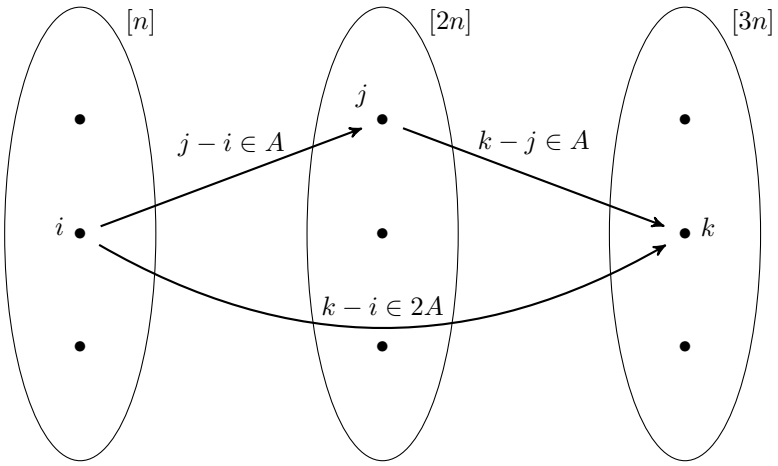
$$(2d-1)^n \leq N < (2d-1)^{n+1}$$

e tente encontrar alguma relação boa com N e d, exclusivamente. (Você consegue ver por que fizemos a outra escolha?)

3 Teoria dos Grafos

Aqui, precisaremos usar a versão finitária. Seja $A \subseteq [n]$ um conjunto sem 3-PAs. Iremos tentar traduzir nosso problema para a linguagem da Teoria dos Grafos.

Para tanto, vamos começar com o conjunto de vértices mais natural $[n]$, e tentaremos definir as arestas utilizando nosso conjunto A. Bem, nosso problema é aditivo, então nada mais natural que definir uma arestas entre i e j quando $i - j$ ou $j - i$ está em A (mais especificamente, quando $|i - j|$ está em A). Porém o módulo não nos permite descrever uma 3-PA por meio de relações entre as arestas. Então vamos adicionar uma assimetria na descrição. Primeiramente, para garantir que as somas estejam sempre em nosso conjunto, vamos considerar conjuntos um pouco maiores: teremos $[2n]$ e $[3n]$ no lugar de $[n]$. Além disso, nós vamos ter três partes disjuntas!



Primeiro, nossas arestas entre duas partes adjacentes são dadas da forma natural como acima. Lembrando que uma 3-PA é uma tripla (a, b, c) tal que $a + c = 2b$, nós vemos que se $j - i = c$ e se $k - j = a$, então $k - i = (k - j) + (j - i) = a + c = 2b$. Logo a forma natural de definir aresta entre as duas cópias não adjacentes é colocando arestas entre k e i se $k - i \in 2A = \{2a \mid a \in A\}$.

Então nosso problema sobre 3-PAs foi traduzido para um problema sobre triângulos e grafos!

3.1 Lema da Regularidade de Szemerédi

Nesta seção, nós veremos que todo grafo (denso) se comporta como um grafo aleatório. Mais especificamente, todo grafo G com uma quantidade suficiente de vértices pode ser separado em poucas partes cujas arestas se comportam de maneira aleatória.

Bem, mas como se comporta um grafo aleatório? Nós vamos começar descrevendo um análogo ao $G(n, p)$. Começamos com dois conjuntos de vértices A e B e colocamos uma aresta entre um vértice de A e um vértice de B com probabilidade $p > 0$. Seja v um vértice qualquer. O valor esperado para $d(v)$ é pn. Quantos vértices possuem grau distante da média pn? Utilizando a desigualdade de Chernoff, é possível demonstrar que, se p é suficientemente grande (ou seja, se nosso grafo é suficientemente denso!)

$$\mathbb{P}\left[|d(v) - pn| > \varepsilon n\right] < 2e^{-cpn}.$$

Porém, não devemos esperar que todos os vértices do nosso se comportem bem, assim, vamos nos voltar a subconjuntos de tamanho não desprezível. Sejam A' um subconjunto de A e B' e um subconjunto de B. Então o valor esperado de arestas entre A' e B' é dado por $p|A'||B'|$, ou ainda, a densidade média de arestas entre A' e B' é $d(A', B') = p$. Como devemos esperar, a maioria dos pares (A', B') tem densidade de arestas próxima a p. Assim, a seguinte noção de pseudoaleatoriedade é natural.

Definição 6

Dizemos que um grafo bipartido (A, B) é ε-regular se para qualquer par (A', B') tais $|A'| \geq \varepsilon|A|$ e $|B'| \geq \varepsilon|B|$ vale

$$|d(A', B') - d(A, B)| < \varepsilon.$$

Desejamos que nosso grafo se comporte como um grafo aleatório. Isto é, desejamos que ele possua as mesmas propriedades que um grafo aleatório possui. Portanto não deve ser surpreendente que a maioria dos vértices possuem grau próximo da média.

Lema 7

Seja (A, B) um par ε-regular de densidade d. Então todos os vértices de A, com exceção de no máximo $2\varepsilon|A|$, têm grau entre $(d - \varepsilon)|B|$ e $(d + \varepsilon)|B|$.

Finalmente, podemos introduzir o tão desejado lema.

Lema 8 (Lema da Regularidade de Szemerédi, 1975)

Sejam $\varepsilon > 0$ e $m \in \mathbb{N}$. Então existe $M(\varepsilon, m) \in \mathbb{N}$ tal que vale o seguinte.

Para qualquer grafo G, existe uma partição de seus vértices $V(G) = A_0 \cup A_1 \cup \cdots \cup A_k$, onde $m \leq k \leq M$ tal que:

- $|A_1| = |A_2| = \cdots = |A_k|$,
- $|A_0| \leq \varepsilon|V(G)|$,
- Todos os pares (A_i, A_j), com exceção de no máximo εk^2, são ε-regulares.

3.2 Lema da Remoção de Triângulos

O lema da remoção de triângulos diz o seguinte: se nós temos poucos triângulos, podemos removê-los todos apagando poucas arestas. Rigorosamente, podemos enunciá-lo da seguinte forma.

Lema 9 (Lema da Remoção de Triângulos, 1976)

Para todo $\varepsilon > 0$, existe $\delta > 0$ tal que, se G é um grafo com no máximo δn^3 triângulos, então é possível remover todos apagando εn^2 arestas.

Vejamos agora como podemos aplicar o Lema da Regularidade ao nosso problema. Seja G um grafo qualquer e $\varepsilon' > 0$ suficientemente pequeno. Podemos tomar uma partição de Szemerédi $V(G) = A_0 \cup A_1 \cup \cdots \cup A_k$. Agora, defina o grafo reduzido $R(G)$ com vértices $\{1, 2, \ldots, k\}$ e arestas entre i e j se e somente se (A_i, A_j) é regular. Pelo Lema 10, se há triângulo em $R(G)$, então há mais que δn^3 triângulos em G, para algum $\delta > 0$. Logo, se G satisfaz a hipótese do Lema da Remoção de Triângulos, então não há triângulos em $R(G)$. Por outro lado, podemos tirar todas as arestas dentro dos A_i's, todas as arestas saindo de A_0 e todas as arestas entre pares não ε-regulares.

Problema. Formalize o argumento acima e demonstre o Lema da Remoção de Triângulos.

3.3 Demonstração

Note, então, que já começamos com $n|A|$ triângulos disjuntos da forma $\{i, i+a, i+2a\}$, onde $i \in [n]$ e $a \in A$. Assim, se $|A| \geq \delta n$, então temos pelo menos δn^2 triângulos disjuntos. Logo precisamos apagar pelo menos δn^2 arestas para remover todos os triângulos. Pelo Lema da Remoção de Triângulos, isso significa que temos pelo menos εn^3 triângulos. Isso implica que há uma 3-PA não trivial para $n > \frac{\delta}{\varepsilon}$.

4 Análise de Fourier

Como é padrão em todas as demonstrações desse resultado, a chave da demonstração reside em separar nosso objeto de estudo em uma parte pseudoaleatória e uma parte pequena/estruturada.

4.1 Pseudoaleatoriedade

Nesta seção, iremos demonstrar a conjectura original de Erdös e Turán. Primeiramente, vamos começar com uma definição que não é padrão na literatura.

Definição 10

Dizemos que uma sequência de conjuntos $A_n \subseteq [n]$ é equidistribuída se a quantidade de números da sequência em cada progressão aritmética só depende da razão, isto é

$$\lim_{N\to\infty} \frac{|A_N \cap (a\mathbb{N}+b)|}{|A_N \cap (a\mathbb{N})|} = 1.$$

para todo a, $b \in \mathbb{N}$. Assim, $|A_N \cap (a\mathbb{N}+b)| \sim \frac{1}{a}|A_N|$.

Essa é a noção de pseudoaleatoriedade que usaremos.

Agora vamos voltar a modelar o nosso problema. Para cada $n \in \mathbb{N}$, seja $R(n)$ um conjunto de tamanho máximo em $[n]$ livre de 3-PAs e seja $r(n)$ sua cardinalidade. Desejamos mostrar que

$$d(n) := \frac{r(n)}{n} \to 0.$$

Primeiramente, note que $\{r(n)\}$ é o que chamamos de uma sequência subaditiva:

$$r(n+m) \leq r(n) + r(m).$$

Isso segue da seguinte observação trivial: $\{u_n\}$ não possui 3-PA se, e somente se, para quaisquer a, $b \in \mathbb{Q}$, $\{au_n + b\}$ não possui 3-PA. Mas a subaditividade nos garante que $d(n)$ converge para algum valor d.

Lema 11 (Lema Subaditivo de Fekete)

Seja $\{s_n\}_{n=1}^{\infty}$ uma sequência subaditiva. Então existe o limite

$$s := \lim_{n\to\infty} \frac{s_n}{n} = \inf_{n\geq 1} \frac{s_n}{n}.$$

Demonstração. Seja s o ínfimo de $\frac{s_n}{n}$. Dado $\varepsilon > 0$, existe $p \in \mathbb{N}$ tal que

$$\frac{s_p}{p} < s + \frac{\varepsilon}{2}.$$

Para qualquer $n \geq p$, existem $q \geq 1$ e $r \leq p$ tais que $n = pq + r$. Seja $M = \max\{s_1, ..., s_{p-1}\}$ e n_0 tal que

$$\frac{M}{n_0} \leq \frac{\varepsilon}{2}.$$

Se $n \geq \max\{p, n_0\}$, então (defina $s_0 = 0$)

$$s \leq \frac{s_n}{n} \leq \frac{q \cdot s_p + s_r}{pq + r} \leq \frac{s_p}{p} + \frac{M}{n_0} \leq s + \varepsilon,$$

de onde segue a existência e o valor do limite. □

Agora vejamos a distribuição dos pares e dos ímpares. Bem, se $u_1, \ldots, u_s$ são os pares em $R(n)$, então $s \leq r(\frac{n}{2})$, pois, dividindo todos os valores por 2, temos uma sequência de números $\leq \frac{n}{2}$ sem 3-PAs. Analogamente, se $v_1, \ldots, v_t$ são os ímpares em $R(n)$, então $s \leq r(\frac{n}{2}) + 1$. Por outro lado, $r(\frac{n}{2}) \sim \frac{1}{2}r(n)$, pois

$$\frac{\frac{1}{2}r(n)}{r(\frac{n}{2})} = \frac{r(n)}{n}\frac{\frac{n}{2}}{r(\frac{n}{2})} \to d \cdot \frac{1}{d} = 1.$$

Logo, a quantidade de ímpares e a quantidade de pares em $R(n)$ é $\sim \frac{1}{2}r(n)$, ou seja, $\frac{dn}{2}$. Assim, vemos que nosso conjunto se comporta mais ou menos como seria esperado que um conjunto aleatório se comportasse (tomando cada número em $[n]$ com probabilidade d).

Problema. Mais geralmente, mostre que a quantidade de números em $R(n)$ da forma $b \pmod a$ é da ordem de $\frac{1}{a}r(n)$, ou seja, $\frac{dn}{a}$.

Lema 12 (Pseudoaleatoriedade)

Com as definições acima,

$$\sum_{k \in R(n)} z^k = d\sum_{k=1}^{n} z^k + o(n)$$

uniformemente em $|z| = 1$.

Para demonstrar esse resultado, precisaremos de uma relação não muito conhecida, que será apresentada na próxima sessão.

Vejamos que, demonstrada essa identidade, nosso problema está resolvido. Um método comum em Teoria dos Números e Combinatória é relacionar problemas aditivos ou recorrências com produtos de séries de potências ou polinômios.

Assim, definindo

$$F(z) = \sum_{k \in R(n)} z^k,$$

vemos que a quantidade de 3-PAs em $R(n)$ é dada pelo coeficiente independente de $F(z)^2F(z^{-2})$ (aqui estamos incluindo as 3-PAs constantes).

O método mais natural para recuperar os coeficientes, visto nos cursos de cálculo, é utilizar a derivada: se $f(z) = \sum_{n=0}^{\infty} a_n z^n$, então $a_n = \frac{f^{(n)}(0)}{n!}$. Porém a derivada não é boa para obter cotas (podemos dizer que o operador derivada não é um *operador limitado*), diferentemente da integral. O leitor que já fez um curso de variáveis complexas deve se lembrar do seguinte resultado.

Teorema 13 (Fórmula Integral de Cauchy)
Seja γ um círculo centrado na origem e orientado no sentido anti-horário e seja $f(z) = \sum_{n=0}^{\infty} a_n z^n$ uma função analítica. Então

$$a_n = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z^{n+1}}\, dz.$$

Assim, a quantidade de 3-PAs em $R(n)$ é dada por

$$P(n) = \frac{1}{2\pi i} \int_\gamma \frac{F(z)^2 F(z^{-2})}{z} dz.$$

Mas, se $f(z) = d\sum_{k=0}^{n-1} z^k$, então $F(z) = f(z) + o(n)$ no círculo unitário S^1, de onde segue que

$$P(n) = \frac{d^3}{2\pi i} \int_\gamma \frac{f(z)^2 f(z^{-2})}{z} dz + o(n^2). \tag{1}$$

Essa conta não é imediata, mas bastante monótona, e foi deixada para o apêndice. Note que aparecerão 8 termos no lado direito, um dos quais será o dominante. Para cotarmos os outros termos, precisaremos de uma ferramente um pouco refinada. O estudo de funções no círculo é conhecido como Análise de Fourier. Aqui, precisaremos apenas de um resultado básico.

Teorema 14 (Teorema de Parseval)
Seja $f(z) = \sum_{n=0}^{\infty} a_n z^n$ uma função tal que $\int_0^1 |f(e^{2\pi i\theta})|^2 d\theta$ é finito. Então

$$\int_0^1 |f(e^{2\pi i\theta})|^2 d\theta = \sum_{n=0}^{\infty} |a_n|^2.$$

Problema. Demonstre o Teorema acima.
Dica: Lembre-se que

$$\int_0^1 e^{2\pi i(m-n)\theta} d\theta = \begin{cases} 1, & \text{se } m = n, \\ 0, & \text{se } m \neq n. \end{cases}$$

O primeiro termo de (1) é a quantidade de 3-PAs em $\{0, 1, ..., n-1\}$. Note que temos $\sim \frac{n}{2}$ 3-PAs começando com 0, $\sim \frac{n}{2}$ 3-PAs começando com 1, ..., e uma única 3-PA começando com $n-1$. Então temos $\frac{n^2}{4} + O(n)$ 3-PAs. Ou seja,

$$P(n) = d^3 \frac{n^2}{4} + o(n^2).$$

Como $R(n)$ só possui as $r(n) = o(n^2)$ PA's constantes, então $d = 0$, concluindo a demonstração.

4.2 O Método do Círculo de Hardy-Littlewood

Seja $p(z)$ um polinômio de grau n e suponha que sabemos o valor de $p(\zeta)$ para algum ζ. Como podemos aproximar $p(z)$ para algum z próximo de ζ? A resposta natural seria utilizando a derivada (ou, mais geralmente, Taylor), mas esse método não é bom para o nosso objetivo, pois desejamos tomar $n \to \infty$. De fato, queremos preservar nossos coeficientes limitados e faremos isso às custas de adicionar alguns polinômios aos jogo.

Dado $p(z)$ um polinômio de grau n, denotamos por $p_k(z)$ o k-ésimo polinômio truncado. Isto é, se $p(z) = \sum_{i=0}^{n} a_i z^i$, então $p_k(z) = \sum_{i=0}^{k} a_i z^i$. A seguinte identidade é válida:

$$p(z) = \left(1 - \frac{z}{\zeta}\right) \sum_{k<n} p_k(\zeta) \left(\frac{z}{\zeta}\right)^k + p(\zeta) \left(\frac{z}{\zeta}\right)^n.$$

Problema. Abra a conta e demonstre essa identidade.

Assim, como z e ζ estarão no círculo unitário, teremos a seguinte cota:

$$|p(z)| \leq |\zeta - z| \sum_{k<n} |p_k(\zeta)| + |p(\zeta)|.$$

Mais especificamente, se $|p_k(\zeta)| \leq M$ para $k = 0, 1, \ldots, n$, então em um arco de comprimento 2ℓ centrado em ζ temos a desigualdade $p(z) \leq M(n\ell + 1)$.

Para demonstrar o Teorema, defina $q(z) = F(z) - f(z)$ e $q_k(z)$ seu truncamento. Nós vamos analisar q_k em pontos bastante especiais dos círculo (as raízes da unidade) e usaremos a identidade acima para transferir a desigualdade para todos os pontos do círculo.

Assim, seja ω uma raiz m-ésima da unidade. Então

$$\begin{aligned} q_k(\omega) &= \sum_{\substack{i \in R(n) \\ i \leq k}} \omega^i - d \sum_{i=1}^{k} \omega^i \\ &= \sum_{a=1}^{m} \omega^a \left(\sum_{\substack{j \in R(n) \\ j \leq k \\ j \equiv a\,(m)}} 1 - d \sum_{\substack{j \leq k \\ j \equiv a\,(m)}} 1. \right) \end{aligned}$$

Note que, embora não são fáceis de comparar entre si, ambos os somatórios estão próximos de $r(\lceil \frac{k}{m} \rceil)$. Mais ainda, note que ambos são $\leq r(\lceil \frac{k}{m} \rceil)$. De fato, se somarmos aos índices do primeiro somatório por $m - a$ e dividirmos por m, então temos uma sequência de termos $\leq \lceil \frac{k}{m} \rceil$ sem 3-PAs. A outra desigualdade segue do fato que $d = \inf \frac{r(n)}{n}$. Para simplificar a notação, defina $r(x) \coloneqq r(\lceil x \rceil)$. Portanto, chamando por s_a o primeiro somatório e t_a o segundo,

$$\begin{aligned} |q_k(\omega)| &= \left| \sum_{a=1}^{m} \omega^a \left(s_a - r\left(\frac{k}{m}\right) \right) + \sum_{a=1}^{m} \omega^a \left(r\left(\frac{k}{m}\right) - dt_a \right) \right| \\ &\leq \sum_{a=1}^{m} \left| s_a - r\left(\frac{k}{m}\right) \right| + \sum_{a=1}^{m} \left| r\left(\frac{k}{m}\right) - dt_a \right| \\ &= \sum_{a=1}^{m} \left(r\left(\frac{k}{m}\right) - s_a \right) + \sum_{a=1}^{m} \left(r\left(\frac{k}{m}\right) - dt_a \right) \\ &= 2m \cdot r\left(\frac{k}{m}\right) - \sum_{a=1}^{m} s_a - dk. \end{aligned}$$

Note agora que $\sum_{a=1}^{m} s_a \geq r(n) - r(n-k) \geq dn - r(n-k)$. Logo

$$\begin{aligned} |q_k(\omega)| &\leq 2m \cdot r\left(\frac{k}{m}\right) - (dn - r(n-k)) - dk \\ &= 2m \left(r\left(\frac{k}{m}\right) - d\frac{k}{m} \right) + [r(n-k) - d(n-k)]. \end{aligned}$$

Lembre-se que queremos uma cota independente de k, para que possamos usar a identidade polinomial, portanto vamos trocar a função $r(n) - dn$ pelo seu parente monótono $f(n) = \sup_{i \leq n}\{f(i) - di\}$.

Como f é claramente monótona, então

$$|q_k(\omega)| \leq 2mf\left(\frac{k}{m}\right) - f(n-k) \leq 2mf\left(\frac{n}{m}\right) + f(n).$$

Além disso, vimos que $r(n) - dn = o(n)$, logo o mesmo é verdade para $f(n)$ (ou seja, $f(n) = o(n)$). Daí seguirá o resultado desejado para as raízes da unidade, resta agora brincarmos (ou sofrermos) com ε e δ para concluirmos a demonstração. Para aproximar bem números no círculo por raízes da unidade, iremos usar o Teorema de Dirichlet.

Teorema 15 (Teorema de Dirichlet)
Seja $N \in \mathbb{N}$ e $z \in S^1$ complexo. Então existe uma raiz m-ésima da unidade ω, com $m \leq N$, tal que

$$|\mathrm{Arg}(z\bar{\omega})| \leq \frac{2\pi}{m(N+1)}.$$

Problema. Procure uma discussão do Teorema de Dirichlet em algum livro e mostre que o enunciado usual é equivalente ao dado acima.

Dado $\varepsilon > 0$, seja n_0 tal que $f(n) < \varepsilon n$ se $n \geq n_0$. Note que queremos cotar não apenas $f(n)$ mas também $mf(\frac{n}{m})$. Então seja n_1 tal que $f(n) < \frac{\varepsilon}{n_0} n$ se $n \geq n_1$. Tomaremos $N = \left\lfloor \frac{n}{n_0} \right\rfloor$ e separaremos em dois casos:

- $m \leq n_0$: Nesse caso, podemos usar apenas a cota trivial (que é suficiente para o que desejamos) $f(\frac{n}{m}) \leq f(n) < \frac{\varepsilon}{n_0} n$, de onde segue que

$$|q_k(\omega)| < 2m\frac{\varepsilon}{n_0} n + \varepsilon n \leq 3\varepsilon n.$$

- $m > n_0$: Como $m \leq N \leq \frac{n}{n_0}$, então $n_0 \leq \frac{n}{m}$ e $f(\frac{n}{m}) < \varepsilon \frac{n}{m}$. Portanto

$$|q_k(\omega)| < 2m\varepsilon\frac{n}{m} + \varepsilon n = 3\varepsilon n.$$

Agora resta mostrar a cota para todos os números no círculo. A conta é semelhante, mas devemos repetir alguns passos. Note que, pelo Teorema de Dirichlet, os arcos centrados nas raízes m-ésimas da unidade, com $m \leq N$ de comprimento $2\frac{2\pi}{m(N+1)}$ cobrem todo o círculo. Assim, tomando $\ell = \frac{2\pi}{m(N+1)}$ e $M = 2mf\left(\frac{n}{m}\right) + f(n)$, segue que

$$|q(z)| \leq M(n\ell + 1) = \left(2mf\left(\frac{n}{m}\right) + f(n)\right)\left(\frac{2\pi n}{m(N+1)} + 1\right).$$

Lembre-se que, como $N = \left\lfloor \frac{n}{n_0} \right\rfloor$, então

$$\frac{2\pi n}{m(N+1)} < \frac{2\pi n_0}{m}.$$

Novamente, nós separaremos em casos:

- $m \leq n_0$: Pelo mesmo argumento de antes

$$\begin{aligned}|q(z)| &\leq \left(2m\frac{\varepsilon}{n_0}n + \frac{\varepsilon}{n_0}n\right)\left(\frac{2\pi n_0}{m} + 1\right)\\ &= 2\pi\frac{n_0}{m}\left(2\frac{m}{n_0}\varepsilon n + \frac{1}{n_0}\varepsilon n\right) + 3\varepsilon n\\ &\leq 4\pi\varepsilon n + 2\pi\varepsilon n + 3\varepsilon n\\ &= (6\pi+3)\varepsilon n.\end{aligned}$$

- $m > n_0$: Aqui não precisamos alterar nada em nossa conta, pois

$$|q(z)| \leq \left(\frac{2\pi n_0}{m} + 1\right) 3\varepsilon n < (6\pi+3)\varepsilon n.$$

Segue, então, que em ambos os casos $|q(z)| < (6\pi+3)\varepsilon n$, ou seja $|q(z)| = o(n)$, como desejávamos.

4.A Cotando integrais

Neste apêndice, iremos cotar três das sete integrais que aparecerão no termo $o(n^2)$ do valor de $P(n)$. Primeiramente, podemos usar apenas o Teorema de Parseval:

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_\gamma \frac{f(z)^2 o(n)}{z}\,dz\right| &= \left|\int_0^1 f(e^{2\pi i\theta})^2 o(n)\,d\theta\right|\\ &\leq \int_0^1 |f(e^{2\pi i\theta})|^2 o(n)\,d\theta\\ &= o(n)\int_0^1 |f(e^{2\pi i\theta})|^2\,d\theta\\ &= o(n)d^2 n\\ &= o(n^2),\end{aligned}$$

mas pode ser necessário utilizar também Cauchy-Schwarz, como na integral abaixo:

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_\gamma \frac{f(z)o(n)^2}{z}\,dz\right| &= \left|\int_0^1 f(e^{2\pi i\theta})(F(e^{2\pi i\theta}) - f(e^{2\pi i\theta}))o(n)\,d\theta\right|\\ &\leq \int_0^1 |f(e^{2\pi i\theta})||F(e^{2\pi i\theta}) - f(e^{2\pi i\theta})|o(n)\,d\theta\\ &= o(n)\int_0^1 |f(e^{2\pi i\theta})||F(e^{2\pi i\theta}) - f(e^{2\pi i\theta})|\,d\theta\\ &\leq o(n)\sqrt{\int_0^1 |f(e^{2\pi i\theta})|^2\,d\theta}\cdot\sqrt{\int_0^1 |F(e^{2\pi i\theta}) - f(e^{2\pi i\theta})|^2\,d\theta}\\ &= o(n^2).\end{aligned}$$

O terceiro caso é semelhante ao primeiro:

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_\gamma \frac{o(n)^3}{z}\,dz\right| &= \left|\int_0^1 (F(e^{2\pi i\theta}) - f(e^{2\pi i\theta}))^2 o(n)\,d\theta\right| \\ &\leq \int_0^1 |F(e^{2\pi i\theta}) - f(e^{2\pi i\theta})|^2 o(n)\,d\theta \\ &= o(n)\int_0^1 |F(e^{2\pi i\theta}) - f(e^{2\pi i\theta})|^2\,d\theta \\ &= o(n^2).\end{aligned}$$

Referências

[1] van der Waerden, B. L. *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk. 15, 212-216, 1927.

[2] van der Waerden, B. L. *How the proof of Baudet's conjecture was found*, Studies in Pure Mathematics (papers presented to R. Rado on the occassion of his 65th birthday, ed. by L. Mirsky, Academic Press), 252-260.

[3] Erdös, P., Turán, P. *On Some Sequences of Integers*, Journal of the London Mathematical Society, 1936.

[4] Roth, K. *On Certain Sets of Integers*, Journal of the London Mathematical Society, 1953.

[5] Szemerédi, E. *On sets of integers containing no four elements in arithmetic progression*, Acta Math. Acad. Sci. Hung, 1969.

[6] Szemerédi, E. *On sets of integers containing no k elements in arithmetic progression*, Acta Arithmetica, 1975.

[7] Fursternberg, H. *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. D'Analyse Math, 1977.

[8] Gowers, T. *A new proof of Szemerédi's theorem*, GAFA, 2001.

[9] Gowers, T. *Hypergraph regularity and the multidimensional Szemerédi theorem*, 2001. Disponível em: https://arxiv.org/abs/0710.3032.

[10] Salem, R., Spencer, D. *On Sets of Integers Which Contain No Three Terms in Arithmetical Progression*, Proc. Natl. Acad. Sci., 1942.

[11] Behreng, F. *On Sets of Integers Which Contain No Three Terms in Arithmetical Progression*, Proc. Natl. Acad. Sci., 1948.

[12] Ruzsa, I. Z., Szemerédi, E. *Triple systems with no six points carrying three triangles*, Combinatorics (Keszthely, 1976), Coll. Math. Soc. J. Bolyai 18, Volume II, 939–945.

[13] Lima, Y. *Szemerédi's Regularity Lemma*, disponível em: http://www.mat.ufc.br/~yuri/szemeredi_regularity_lemma.pdf.

[14] Newman, D. *Analytic Number Theory*, New York, Springer, 2000.

[15] Zhao, Y. *Graph Theory and Additive Combinatorics*, 2020. Disponível em: http://yufeizhao.com/gtac/.