COBERTURAS DISTINTAS DOS INTEIROS

Será que existem coberturas dos números inteiros por congruências distintas em que as progressões aritméticas não se intersetam e que sejam também exatas? Será que existem coberturas por congruências distintas com módulo mínimo arbitrariamente grande? Vamos tentar responder a estas questões.

PEDRO J. FREITAS
Universidade de Lisboa
pedro@ptmat.fc.ul.pt

MANUEL SILVA
Universidade Nova de Lisboa
mnas@fct.unl.pt

ORIGEM DO PROBLEMA

Em 1849, Polignac conjeturou erradamente que todos os números ímpares $n \geq 3$ podiam ser escritos na forma $n = 2^k + p$, com p primo e k inteiro positivo, i.e., soma de uma potência de 2 e um número primo. 127 e 959 são dois exemplos de números ímpares que não podem ser escritos na forma anterior. Em 1934, Romanoff mostrou que os números naturais da forma $2^k + p$ têm densidade positiva. Dizemos que um conjunto infinito $A \subset \mathbb{N}$ tem densidade positiva se o número de elementos de A no intervalo $[1, N]$ é, pelo menos, cN, para uma certa constante $0 < c < 1$. Numa carta a Erdös, no mesmo ano, colocou ainda a seguinte questão: será que existem infinitos números ímpares que não podem ser escritos na forma $2^k + p$? Em 1950, Erdös encontrou uma progressão aritmética de números ímpares nenhum dos quais é soma de uma potência de 2 e um número primo. Na resolução deste problema, Erdös introduziu o conceito de cobertura por congruências, que iremos descrever a seguir.

Comecemos pelo conceito, bem conhecido, de congruência ou resto. Dois números inteiros, a e b, dizem-se congruentes módulo um inteiro positivo m se deixam o mesmo resto na divisão por m. Usando a notação introduzida por Gauss, escrevemos $a \equiv b \pmod{m}$. Por exemplo, $11 \equiv 20 \pmod{3}$, porque deixam ambos resto 2 quando divididos por 3. O conjunto de inteiros numa dada classe de congruência forma uma progressão aritmética. Por exemplo, os inteiros positivos n que satisfazem $n \equiv 2 \pmod{5}$ são os seguintes: $2, 7, 12, \cdots$, ou seja, uma progressão aritmética de razão 5.

Vamos agora tentar obter coberturas dos inteiros como união de progressões aritméticas ou classes de congruência. Se usarmos o mesmo módulo, a tarefa não é difícil... Sabemos que resto da divisão de um número inteiro por 3 pode ser 0, 1 ou 2. Logo, o sistema de congruências: $\{0 \bmod 3, 1 \bmod 3, 2 \bmod 3\}$ é certamente uma cobertura dos inteiros. Todo o inteiro satisfaz, pelo menos, uma das condições anteriores.

E se exigirmos que as razões das progressões aritméticas, ou módulos das congruências, sejam distintas, será que existem coberturas dos inteiros neste caso? Sim, de facto, existem. O exemplo mais simples de cobertura por congruências distintas é o seguinte:

$\{0 \bmod 2, 0 \bmod 3, 1 \bmod 4, 5 \bmod 6, 7 \bmod 12\}$.

O mínimo múltiplo comum dos módulos das congruências envolvidas é 12. Deste modo, para verificar que todo o número inteiro satisfaz, pelo menos, uma destas congruências, basta ver que tal acontece para os inteiros $1 \leq n \leq 12$. Deixamos esta tarefa ao leitor mais desconfiado.

COBERTURAS EXATAS

No exemplo anterior, de cobertura por congruências distintas, algumas das progressões aritméticas intersetam-se, i.e, certos números inteiros satisfazem simultaneamente duas, ou mais, congruências: 6 satisfaz as duas primeiras congruências, porque é múltiplo de 2 e 3. Va-

mos designar por *cobertura exata* uma cobertura dos inteiros em que as progressões aritméticas não se intersetam. O primeiro exemplo de cobertura $\{0,1,3 \pmod 3\}$ tem esta propriedade. Apetece perguntar se isto é evitável, ou seja, será que existem coberturas por congruências distintas dos números inteiros em que as progressões aritméticas não se intersetam e que sejam também exatas? Sem dúvida, uma boa pergunta, colocada oportunamente por Erdös. Na verdade, não existem coberturas por congruências que sejam simultaneamente distintas e exatas. A prova deste facto é demasiado bela para não ser partilhada.

Teorema 1. (Mirsky e Newman) *Se os números naturais podem ser obtidos como união de um número finito (pelo menos, duas) de progressões aritméticas, então, duas destas progressões aritméticas têm a mesma razão.*

A cada conjunto de números naturais podemos associar uma função geradora, que não é mais do que uma série de potências, em que os expoentes coincidem com os elementos do conjunto de partida. Deste modo, a cada uma das progressões aritméticas $\{a+nb : n \in \mathbb{N}\}$ corresponde a função geradora:

$$z^a + z^{a+b} + z^{a+2b} + \cdots = \frac{z^a}{1-z^b}.$$

Suponhamos que os inteiros positivos resultam de uma certa união disjunta de k progressões aritméticas: $\{a_i + nb_i\}, i = 1,2,\cdots,k$, cujas razões $b_1, b_2, \cdots, b_k$ são todas distintas. Uma vez que a função geradora dos números naturais é simplesmente

$$1 + z + z^2 + z^3 + \cdots = \frac{1}{1-z},$$

obtemos a seguintes igualdade:

$$\frac{1}{1-z} = \frac{z^{a_1}}{1-z^{b_1}} + \frac{z^{a_2}}{1-z^{b_2}} + \ldots + \frac{z^{a_k}}{1-z^{b_k}}.$$

Podemos supor que z é um número complexo com $|z| < 1$, para garantir a convergência das séries de potências, e que b_k é maior do que b_i, sempre que $i < k$. Agora um pouco de magia. Fazemos tender a variável complexa z para $\epsilon = e^{2\pi i/b_k}$. Observamos que $\epsilon^{b_k} = 1$ mas $\epsilon \neq 1$ e $\epsilon^{b_i} \neq 1, 1 \leq i < k$. A função do lado esquerdo tende para um valor finito. Além disso, todas as parcelas do lado direito tendem para um valor finito, exceto a última, que tende para infinito, logo, a função do lado direito tende para infinito, o que é uma contradição! Observe-se que a não existência de uma cobertura exata distinta para os números naturais implica facilmente a não existência de tal cobertura para os números inteiros.

CONJETURA DO MÓDULO MÍNIMO

Vamos agora descrever um problema, que Erdös gostava de designar como um dos seus problemas preferidos. Erdös atribuiu um valor monetário de 1000 dólares para a resolução desta conjetura. Este é um dos valores mais altos na classificação de Erdös.

Na cobertura por congruências distintas apresentada anteriormente, podemos observar que a classe de congruência com módulo menor é 2.

Será possível obter uma cobertura com as mesma características (congruências distintas) em que o módulo mínimo seja 3? Também neste caso é possível. O seguinte exemplo é de Erdös: 0 mod 3, 0 mod 4, 0 mod 5, 1 mod 6, 1 mod 8, 2 mod 10, 11 mod 12, 1 mod 15, 14 mod 20, 5 mod 24, 8 mod 30, 6 mod 40, 58 mod 60, 26 mod 120.

Será ainda verdade que exista uma cobertura por congruências distintas, cujo módulo mínimo seja 4? A resposta volta a ser positiva. Pace Nielsen (2009) encontrou uma cobertura por congruências distintas, cujo módulo mínimo é 40. Erdös conjeturou que deveriam existir coberturas dos inteiros por congruências distintas com módulo mínimo arbitrariamente grande.

Conjetura. (Erdös 1950) *Para qualquer $N > 1$, existe uma cobertura por congruências distintas,*

$$\{a_i \pmod{m_i}\}, 1 \leq i \leq k,$$

tal que $m_i > N$ para $1 \leq i \leq k$.

Será que o módulo mínimo pode, de facto, ser tão grande como se queira? O matemático Bob Hough demonstrou recentemente que esta conjetura é, na verdade, falsa. O seu resultado estabelece mesmo um majorante uniforme para o valor do módulo mínimo.

Teorema 2. (Hough 2015) *O módulo mínimo numa cobertura dos inteiros por congruências distintas não excede* 10^{16}.

A demonstração envolve dois ingredientes essenciais. Para obter um majorante explícito do módulo mínimo, foi utilizada uma estimativa relacionada com a distribuição dos números primos. O segundo ingrediente, algo inesperado, é o uso do famoso Lema Local de Lovász, considerado um dos resultados mais importantes no âmbito do método probabilístico desenvolvido por Erdös. Numa resolução de um problema matemático interessante, especialmente em Combinatória, o mais provável é que o método usado na demonstração seja totalmente inesperado.

Ainda existem diversos problemas por resolver sobre coberturas dos inteiros por congruências. Terminamos

com dois problemas abertos e um desafio simples.

Conjetura (Erdös e Selfridge). *Não existem coberturas por congruências distintas dos números inteiros com todos os módulos ímpares.*

Conjetura (Schinzel). *Dada uma cobertura por congruências dos números inteiros* $a_i \pmod{n_i}$ *com* $1 \leq i \leq r$, *existe sempre* $i \neq j$ *tal que* $n_i | n_j$.

A conjetura de Schinzel resulta, de modo nada evidente, da conjetura dos módulos ímpares. Deixamos um desafio ao leitor: construir uma cobertura por congruências distintas dos números inteiros com todos os módulos pares. Pode tentar modificar um dos exemplos de coberturas distintas dado neste texto.

REFERÊNCIAS

[1] P. Erdös, "On integers of the form $2^k + p$ and some related problems", *Summa Brasil. Math.* 2 (1950), 113–123.

[2] Bob Hough. "Solution of the minimum modulus problem for covering systems", *Annals of Math 181*, n. 1 (2015): 361-382.