Combinatória: Um conjunto de técnicas

1. Um problema inicial: o problema dos elevadores

O seguinte problema foi proposto, no dia 16/07/2003, na lista de discussão da OBM (veja como entrar nessa lista no site da OBM: `http://www.obm.org.br`).

Num prédio de apartamentos há 7 elevadores que páram em não mais que 6 andares. É possível ir de um andar a qualquer outro sem trocar de elevador. Qual é o número máximo de andares que esse prédio pode ter?

No dia seguinte, o professor Nicolau Saldanha deu a seguinte resposta:

O problema é bem legal. Ainda não completei uma solução mas vou mandar meus resultados parciais.

$N \le 14$

De fato, temos no máximo 42 paradas (uma parada é um par (i, j) onde i é um andar, j é um elevador, e o elevador j pára no andar i). Se $N > 11$ devemos ter pelo menos três paradas por andar (pois duas paradas nos dão apenas dois elevadores que atingem no máximo 10 outros andares). Assim $3N \le 42$ e $N \le 14$.

$N \ge 12$

Basta observar a configuração abaixo onde um `+` *indica que o elevador pára naquele andar e um* `.` *indica que ele não pára. Os andares estão um em cima do outro, claro, e os elevadores um ao lado do outro. Observe que 6 elevadores foram suficientes.*

```
+++...
+++...
+++...
+..++.
+..++.
+..++.
.+.+.+
.+.+.+
.+.+.+
..+.++
..+.++
..+.++
```

Eu fiz uns diagramas e me convenci que $N \le 13$ mas a prova foi meio braçal, no caso a caso, e pode estar errada.

[]s, N.

De fato, estava. No dia 18, o professor Carlos Moreira (Gugu) apresentou uma solução com 14 andares:

Oi Nicolau,

Acho que consegui uma solucao com 14 andares: é que $P := P_2(Z/(2))$ tem 7 elementos e 7 retas (seja R o conjunto de suas retas). Tomamos como conjunto dos andares $P \times \{0, 1\}$, e como conjunto dos elevadores a diagonal de $R \times R$.

Dá para escrever mais explicitamente isso: os andares são $1, 2, \ldots, 14$. Os elevadores são $\{1, 2, 3, 8, 9, 10\}$, $\{1, 4, 5, 8, 11, 12\}$, $\{1, 6, 7, 8, 13, 14\}$, $\{2, 4, 6, 9, 11, 13\}$, $\{2, 5, 7, 9, 12, 14\}$, $\{3, 4, 7, 10, 11, 14\}$ e $\{3, 5, 6, 10, 12, 13\}$.

Abraços,

Gugu

1.1. Parêntesis teórico

$P_2(Z/(2))$ é o plano projetivo de ordem 2. Um *plano projetivo* é um conjunto de pontos e retas que satisfazem as seguintes condições:

(i) Por dois pontos quaisquer passa exatamente uma reta.

(ii) Duas retas quaisquer interceptam-se em exatamente um ponto.

(iii) Existem quatro pontos três a três não colineares.

Um plano projetivo pode ter um número finito de pontos (e, portanto, cada reta tem um número finito de pontos também). A solução apresentada por Gugu se baseia nas seguintes figuras:

Mais sobre o assunto pode ser encontrado na referência [1] (e em suas referências!).

1.2. Voltando...

Mais tarde, no mesmo dia, em resposta a Domingos Jr., Gugu mandou outra mensagem à lista:

Caro Domingos,

Você pode esquecer as minhas três primeiras linhas: elas só servem como explicação de como eu cheguei a essa solução (e aliás não estão bem escritas: eu devia ter dito que o conjunto dos elevadores (ou, mais propriamente, o conjunto dos conjuntos de andares nos quais pára cada elevador) é $\{(r \times \{0\}) \cup (r \times \{1\}), r \in R\}$*).*

Nas três linhas seguintes eu descrevo uma solução explícita com 14 andares, listando os conjuntos de andares em que pára cada elevador. Essa solução não é única: dada qualquer permutação de $\{1, 2, ..., 14\}$*, podemos aplicar essa permutação a todos os elementos de todos os conjuntos que eu listei e obter outra solução. Isso dá muitas soluções (mas não sei se é possível classificar todas as soluções de um jeito simples usando esse tipo de equivalência).*

Abraços,

Gugu

1.3. Um problema foi resolvido. Mas...

Foi aí que entrei (na verdade, esse foi o primeiro dos emails que li sobre o assunto, na manhã do dia 19). Recentemente, eu estudei planos projetivos finitos e block designs e esse problema me interessou. De repente, eu me perguntei:

Problema. *Quantas soluções existem? Será que existe alguma solução que não tem a ver com planos projetivos?*

Mandei em seguida um email cheio de referências sobre um outro problema que julguei ser relacionado e fiz uma tentativa de contagem de soluções. Infelizmente, o problema não era tão relacionado assim e a contagem estava errada.

Assim, pensei no problema mais seriamente um pouco antes, durante e após o almoço daquele dia (sim, eu pensei durante o almoço – e minha família também achou esquisito). Depois de uma hora, cheguei a um resultado, que apresento a seguir.

1.4. Passo 1: Contagem dupla e pombos atacam!

A idéia é tentar encontrar todos os exemplos para $N = 14$. Do que o professor Nicolau comentou, devem passar pelo menos três elevadores em cada andar. Nesse caso, há exatamente $6 \times 7 = 42$ paradas de elevadores para 14 andares. Observe que $42 = 14 \times 3$, ou seja, o número de paradas dá "certinho" para os andares, de modo que por cada andar passam **exatamente** 3 elevadores. Um modo mais formal de se escrever isso é supor que um andar "guloso" é servido por mais de três elevadores e chegar a um absurdo.

O que acabamos de fazer foi usar dois princípios bastante importantes em problemas desse tipo.

O primeiro princípio foi contar o total de paradas (elevadores vezes andares por elevador) e pensar nelas de modo diferente (andares e elevadores por andar). Apresentamos o

Princípio Importante 1: Contagem Dupla

Sejam P e Q conjuntos finitos e $S \subset P \times Q$. Se $|A|$ denota a cardinalidade do conjunto A, então

$$\sum_{p \in P} |\{q \mid (p;q) \in S\}| = \sum_{q \in Q} |\{p \mid (p;q) \in S\}|$$

Traduzindo: o total de elementos de uma parte S de um produto cartesiano de dois conjuntos P e Q não muda se contarmos fixando elementos de P e somando ou fixando elementos de Q e somando. No nosso problema, P é o conjunto dos elevadores e Q é o conjunto de andares. S é o conjunto das paradas (i, j) na qual (i, j) pertence a S quando o elevador i pára no andar j.

Em casos mais complicados, vale a pena construir uma tabela (que, no fundo, é uma representação do produto cartesiano). Mas você pode pensar nesse princípio de um modo mais intuitivo (e, digamos, "político"):

Princípio Importante 1: Contagem Dupla (intuitivo)

Quando há dois conjuntos de coisas relacionados, veja tal relação do ponto de vista de cada conjunto.

Observe que a média de elevadores que passam em cada andar é $42/14 = 3$ e que passam pelo menos 3 elevadores em cada andar. De modo geral, se uma variável é sempre maior (menor) que ou igual a um número M e sua média é igual a M, então a variável é sempre igual a M.

De certo modo, esse fato é relacionado a outro princípio importante, que é o *Princípio da Casa dos Pombos*:

Princípio Importante 2: Casa dos Pombos

Se há $n+1$ pombos para serem distribuídos em n casas, então há pelo uma casa com pelo menos dois pombos.

A relação não parece óbvia, mas transparece um pouco mais na seguinte formulação:

Princípio da Casa dos Pombos (formulação com médias)

Se uma variável tem média igual a M, então existe a variável assume pelo menos um valor maior ou igual a M e pelo menos um valor maior ou igual a M.

Na verdade, você pode pensar intuitivamente no Princípio da Casa dos Pombos da maneira a seguir, que pode ajudar a identificar problemas em que devemos aplicar esse princípio e é mais simples de lembrar.

> **Princípio Importante 2: Casa dos Pombos (intuitivo)**
>
> Se há muitos pombos para poucas casas, alguma casa vai ter muitos pombos. E se há poucos pombos para muitas casas, haverá uma (ou até muitas!) casa(s) vazia(s).

1.5. Passo 2: Elevadores aos pares – contagem dupla, pombos, e um pouco de força bruta

Tendo em vista o exemplo baseado em geometria projetiva do Gugu, comecei a pensar geometricamente. Problemas nos quais há conjuntos e se pensa muito em interseções e coisas do tipo "quaisquer dois estão contidos em um mesmo conjunto" podem ser traduzidos em termos da geometria. Alguns fatos são mais fáceis de se enxergar sob um ponto de vista geométrico.

Assim, comecei a pensar nos elevadores como retas e nos andares como pontos. O próximo passo foi pensar nas interseções entre retas e número de retas passando por dois pontos fixados (nesses problemas, nem sempre – aliás, quase nunca! – duas retas se interceptam em no máximo dois pontos e dois pontos determinam uma única reta). No nosso problema, as interseções de dois elevadores são os andares que são servidos por ambos e o número de retas passando por dois andares fixados é o número de elevadores que ligam esses andares.

Às vezes, é interessante pensar na interseção média de dois elevadores (veja o princípio importante 2: casa dos pombos!). Veja que a nossa média é sobre *pares* de elevadores, que são no total $\binom{7}{2} = \frac{7 \cdot 6}{2} = 21$. Uma interseção, como vimos no parágrafo anterior, é caracterizada por um andar comum a dois elevadores. Vendo do ponto de vista dos elevadores, não podemos concluir muita coisa. Mas, vendo do ponto de vista dos andares (veja o princípio importante 1: contagem dupla), podemos ver que cada andar pertence a $\binom{3}{2} = 3$ elevadores (usaremos os termos de pertinência e incidência de geometria livremente no texto), assim há $14 \cdot 3 = 42$ interseções. A média de interseções por par de elevadores é $\frac{42}{21} = 2$.

Agora, vejamos se podemos encontrar as possíveis quantidades de interseções entre dois elevadores. Nossa estratégia é estudar um pouco caso a caso. Nessa hora é importante trabalhar de modo mais estruturado possível. Em algumas aulas, eu fiquei surpreso ao saber que alguns (ótimos) alunos achavam que a Combinatória é sempre algo desestruturado. Talvez isso se deva ao fato de que normalmente o que se vê em Combinatória é um conjunto de técnicas aparentemente pouco relacionadas entre si, enquanto outras áreas, como Teoria dos Números, por exemplo, tem uma estrutura bastante seqüencial (para uma discussão bastante interessante sobre as duas culturas matemáticas – "construtores de teoria" e "resolvedores de problemas" – veja a referência [2]).

> **Princípio Importante 3: Trabalhar de modo estruturado**
>
> Ao estudar casos, trabalhe de modo estruturado:
>
> (a) Estabeleça uma ordem na hora de estudar casos. Assim você saberá quando os casos terminam;
>
> (b) Reduza casos *supondo sem perda de generalidade* e observando que um caso é *análogo* a outro;
>
> (c) Procure padrões que possam ser generalizados.

Eu costumo comparar a enumeração de casos com duas experiências da infância: uma é catar bolinhas de gude espalhadas na sala de estar (você acha uma ali, outra aqui, mas nunca sabe se tem mais alguma por aí); outra é guardar dominós (você guarda a peça 0-0, depois a 0-1. depois a 0-2... 1-1, 1-2, ..., 2-2, ... – pelo menos eu sempre guardei meus dominós nessa ordem). Você pode pensar no princípio importante 3 assim: "Às vezes, você tem que catar bolinhas de gude, mas sempre que for possível, guarde dominós."

Assim, suponhamos, sem perda de generalidade, que os elevadores 1, 2 e 3 passam pelo andar 1. Suponha também que o elevador 1 passa pelos andares 1, 2, 3, 4, 5 e 6. Eu tinha feito a seguinte tabela no meu papel quadriculado:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	×	×	×	×	×	×								
2	×													
3	×													
4														
5														
6														
7														

Nessa tabela, as linhas são os elevadores e as colunas são os andares. Marcamos um $\times$ numa casa da tabela quando o elevador da linha passa no andar da coluna.

Observe que os elevadores 1, 2 e 3 devem ser suficientes para se ir do andar 1 para qualquer outro. Falta definir, em cada uma das linhas 2 e 3, mais cinco $\times$. Como faltam os andares 7 a 14 (8 no total) para se chegar do andar 1 e devemos marcar um total de 10 $\times$'s, podemos ter no máximo $10 - 8 = 2$ repetições. Assim, a interseção entre 1 e 2 deve ter, no máximo, três andares, não podendo, assim, ter mais que três andares.

Suponhamos que essa interseção tenha exatamente três andares (note que só agora estamos dividindo o problema em casos pela primeira vez!) e que esses sejam 1, 2 e 3 (não perdemos generalidade aqui). Suponhamos, também, que os outros andares do elevador 2 sejam 7, 8, 9 (também não perdemos generalidade aqui!).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	×	×	×	×	×	×								
2	×	×	×				×	×	×					
3	×													
4														
5														
6														
7														

O elevador 3 deve passar pelos andares 10 a 14, para que possamos vir do andar 1.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	×	×	×	×	×	×								
2	×	×	×				×	×	×					
3	×									×	×	×	×	×
4														
5														
6														
7														

Agora, viremos nossa atenção ao andar 2. Dele, utilizando os elevadores 1 e 2, podemos ir aos andares 1, 3, 4, 5, 6, 7, 8 e 9. Faltam os andares de 10 a 14. Suponhamos (novamente sem perda de generalidade) que o terceiro elevador que passa pelo andar 2 é o elevador 4. Ele deve passar pelo andar 2 e pelos andares 10 a 14. Mas isso não é possível, pois isso implica os elevadores 2 e 3 terem interseção com mais que três andares.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$								
2	$\times$	$\times$	$\times$				$\times$	$\times$	$\times$					
3	$\times$									$\times$	$\times$	$\times$	$\times$	$\times$
4		$\times$								$\times$	$\times$	$\times$	$\times$	$\times$
5														
6														
7														

Assim, não é possível termos um par de elevadores com interseção de tamanho maior que dois. Mas a média de interseções entre um par de elevadores é 2! Assim, todo par de elevador tem interseção de dois elementos.

1.6. Passo 3: Pareando os pares

Agora, suponha, sem perda de generalidade, que os elevadores 1 e 2 passam pelos andares 1 e 2. Suponha também que o elevador 1 passa pels andares 1 a 6 e o elevador 2 passa pelos andares 1, 2, 7 a 10. Pensando no terceiro elevador (que supomos ser o 3) do andar 1, ele deve passar pelos andares 11 a 14.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$								
2	$\times$	$\times$					$\times$	$\times$	$\times$	$\times$				
3	$\times$										$\times$	$\times$	$\times$	$\times$
4														
5														
6														
7														

Falta um $\times$ para colocar na terceira linha.

Pensemos agora no andar 2. Podemos, com os elevadores 1 e 2, ir de lá aos andares 1 e 3 a 10. Faltam 11 a 14. O elevador 3 passa por lá e parece ser útil e agradável colocar o último $\times$ na coluna 2. Na verdade, é a única possibilidade: se um outro elevador diferente passasse pelo andar 2, ele teria interseção de tamanho pelo menos 4 com o elevador 3, o que não pode acontecer.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$								
2	$\times$	$\times$					$\times$	$\times$	$\times$	$\times$				
3	$\times$	$\times$									$\times$	$\times$	$\times$	$\times$
4														
5														
6														
7														

Chegamos, então, ao seguinte resultado: se dois elevadores passam por dois andares em comum, então o terceiro elevador que passa por um desses andares também passa pelo outro.

Com isso, podemos formar pares de andares que correspondem a interseções de elevadores.

1.7. Passo 4: Olha o plano projetivo aí, gente!

Feito isso, não fica tão complicado terminar: temos 7 pares de andares e 7 elevadores. Cada elevador contém 3 pares de andares. Dois elevadores têm exatamente um par em comum. Por dois pares passa exatamente um elevador. Só pode ser o plano projetivo no qual os pontos são pares de andares e os elevadores são as retas.

Ou seja, a solução que o Gugu apresentou é, essencialmente, a única. Na verdade, de certo modo isso não é tão surpreendente assim. Muitos (mas não todos) planos projetivos podem ser baseados em corpos, que são estruturas da Álgebra que "dão muito certo". Assim, em situações em que as coisas "dão muito certo", geralmente construímos exemplos baseados em estruturas baseadas em corpos (no nosso caso, planos projetivos).

1.8. Passo 5: Fazendo a contagem final

Agora que sabemos como são as soluções, podemos contá-las. O total não é tão simples de contar e achei interessante calcular aqui e mostrar algumas técnicas importantes de contagem.

Os modelos de contagem vistos no ensino médio são, no fundo, mais uma prova de que contagem pode ser algo estruturado. Por exemplo, o princípio fundamental da contagem é uma aplicação de produto cartesianos: se você tem 3 calças (uma azul-marinho, outra azul-turquesa e outra azul-bebê) e 2 camisas (uma amarelo-limão e outra verde-lima), há 3×2 maneiras de se escolher uma calça e uma camisa. A escolha pode ser interpretada como um par ordenado (calça;camisa) do produto cartesiano $A \times B$, em que A é o conjunto das calças e B é o conjunto das camisas.

Agora, vamos à nossa contagem. Faremos o seguinte: primeiro calcularemos o número de maneiras de rotular (identificar) os pontos e as retas de um plano projetivo de ordem 2 e depois o número de maneiras de distribuirmos os andares em sete pares rotulados.

A *matriz de adjacência* do nosso plano projetivo é uma matriz $A = (a_{ij})_{7\times 7}$ (cada linha corresponde a um ponto e cada coluna, a uma reta). Se o ponto i pertence à reta j, $a_{ij} = 1$. Caso contrário, $a_{ij} = 0$. Devemos ter três uns em cada linha e cada coluna. Um exemplo de matriz de adjacência é

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Podemos escolher as posições dos uns da primeira linha de $\binom{7}{3}$ maneiras. Tome o primeiro $a_{1j} = 1$ da primeira linha. Nessa coluna j podemos escolher os dois demais uns de $\binom{6}{2}$ maneiras. Digamos que esses uns são a_{mj} e a_{nj}, $m < n$. Mostramos uma matriz parcialmente preenchida a seguir.

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & & & & & & \\ 1 & & & & & & \\ 0 & & & & & & \\ 0 & & & & & & \\ 0 & & & & & & \\ 0 & & & & & & \end{pmatrix}$$

Note que os elementos da matriz delimitados pelos uns que já colocamos devem ser todos nulos (no nosso exemplo, $a_{22} = a_{23} = a_{32} = a_{33} = 0$ pois a reta 1 é a única que passa pelos pares de pontos $\{1;2\}$, $\{1;3\}$ e $\{2;3\}$). Podemos, então, escolher os demais uns da linha m de $\binom{4}{2}$ maneiras. Note que isso determina os uns da linha n (nas colunas onde não colocamos um nas linhas 1 e m).

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & & & & & & \\ 0 & & & & & & \\ 0 & & & & & & \\ 0 & & & & & & \end{pmatrix}$$

Seja k e ℓ o segundo e o terceiro uns da primeira linha. Analogamente ao que fizemos com as colunas, há $\binom{4}{2}$ maneiras de escolhermos os uns da coluna k, determinando os uns da coluna ℓ.

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & & & & \\ 0 & 1 & 0 & & & & \\ 0 & 0 & 1 & & & & \\ 0 & 0 & 1 & & & & \end{pmatrix}$$

Falta preencher o que corresponderia ao quadrado 4×4 no canto inferior direito da matriz acima. Observe a linha 4 dessa matriz. Precisamos colocar mais 2 uns nessa linha, mas não podemos escolher os pares de colunas $\{4; 5\}$ e $\{6; 7\}$, de modo que há $\binom{4}{2} - 2 = 4$ maneiras de se fazer essa escolha. Novamente, essa escolha determina as posições dos uns na linha 5.

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & & & & \\ 0 & 0 & 1 & & & & \end{pmatrix}$$

Por fim, falta 1 um na coluna 4. Podemos escolher sua posição de 2 maneiras. E isso determina o resto da matriz:

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Assim, pelo princípio multiplicativo, o número de matrizes de adjacência possíveis é

$$\binom{7}{3} \cdot \binom{6}{2} \cdot \binom{4}{2} \cdot \binom{4}{2} \cdot 4 \cdot 2 = 151200$$

1.9. Outra maneira de contar

Podemos contar o número de matrizes de adjacência de outa maneira. Há 7! maneiras de distribuir as retas entre as colunas e 7! maneiras de distribuir os pontos entre as linhas. Mas podemos ver, por exemplo, que as escolhas

$$\begin{array}{cc} & \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} & \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \end{array} \quad \text{e} \quad \begin{array}{cc} & \begin{array}{ccccccc} 1 & 3 & 2 & 4 & 5 & 7 & 6 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 6 \\ 7 \\ 4 \\ 5 \end{array} & \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

representam o mesmo plano projetivo e, portanto, têm a mesma matriz de adjacência. Assim, devemos dividir $7! \cdot 7!$ pelo número de repetições como a que mostramos acima.

O número de repetições é igual ao número de maneiras de associarmos números aos pontos da figura a seguir de modo que as retas sejam, digamos, $\{1;2;3\}$, $\{1;4;5\}$, $\{1;6;7\}$, $\{2;4;6\}$, $\{2;5;7\}$, $\{3;4;7\}$ e $\{3;5;6\}$ (podemos supor isso sem perda de generalidade).

Há 7 maneiras de escolhermos quem vai ser o ponto 1 e 6 maneiras de escolhermos quem vai ser o ponto 2. Com isso, determinamos quem vai ser o ponto 3 (é o outro ponto da reta que passa pelos pontos 1 e 2). Sobram quatro pontos. Podemos escolher qualquer um para ser o ponto 4 e determinamos o ponto 5 (é o outro ponto da reta que passa por 1 e 4), o ponto 6 (o outro ponto da reta que passa por 2 e 4) e o ponto 7 (é o que sobrou!). Logo há $7 \cdot 6 \cdot 4 = 168$ repetições e o total de matrizes é $7!7!/168 = 151200$. A propósito: essas repetições são chamadas *colineações* em geometria projetiva.

Aliás, fica como exercício para você provar que um plano projetivo de ordem p, p primo, tem $(p^2+p+1)(p^2+p)p^2(p-1)^2$ colineações.

1.10. Terminando o problema...

Além disso, há $7!$ maneiras de distribuir os elevadores entre as colunas da matriz e $14!/(2!)^7$ maneiras de distribuir os andares em pares entre as linhas da matriz, de modo que o total de soluções desejado é

$$151200 \cdot 7! \cdot \frac{14!}{2^7} = 519015956659200000$$

2. Bijeções e Funções Geratrizes: o Problema 6 da IMO 1995

O problema 6 da IMO 1995 era:

Seja p um número primo ímpar. Determine o número de subconjuntos de $\{1;2;3;\ldots;2p\}$, com p elementos cuja soma é divisível por p.

Note que o problema envolve um número p primo, o que sugere que façamos uso de conhecimentos em outras áreas, como Teoria dos Números e Álgebra (os números $\text{mód } p$ formam um corpo). Há duas maneiras de resolver esse problema.

2.1. Solução 1: Bijeções e um pouco de Teoria dos Números

O que impera a contagem é o que chamamos de *bijeção*. Grosso modo, uma bijeção é uma associação que liga cada elemento de um conjunto a um elemento do outro, de modo que para cada elemento de um conjunto existe um único elemento do outro conjunto associado a ele e vice-versa (sim, bijeções são funções!). Um fato importante é que se existe uma bijeção entre dois conjuntos estão ambos têm o mesmo número de elementos.

Só que em certos casos encontrar bijeções dá certo trabalho. Vamos estudar alguns casos pequenos de números primos ímpares p.

Vejamos $p = 3$. Há $\binom{6}{3} = 20$ subconjuntos de $\{1; 2; 3; 4; 5; 6\}$ com 3 elementos. Vamos classificá-los em classes de subconjuntos de soma que deixam restos 0, 1 e 2 quando divididos por 3:

Resto 0	Resto 1	Resto 2
$\{1; 2; 3\}$	$\{1; 2; 4\}$	$\{1; 2; 5\}$
$\{1; 2; 6\}$	$\{1; 3; 6\}$	$\{1; 3; 4\}$
$\{1; 3; 5\}$	$\{1; 4; 5\}$	$\{1; 4; 6\}$
$\{1; 5; 6\}$	$\{2; 3; 5\}$	$\{2; 3; 6\}$
$\{2; 3; 4\}$	$\{2; 5; 6\}$	$\{2; 4; 5\}$
$\{2; 4; 6\}$	$\{3; 4; 6\}$	$\{3; 5; 6\}$
$\{3; 4; 5\}$		
$\{4; 5; 6\}$		

Se estudarmos $p = 5$, obtemos 52 subconjuntos com soma divisível por 5 e 50 subconjuntos das demais quatro classes (para estudar esse caso você precisa fazer uma contagem um pouco mais estruturada).

Isso nos leva a conjecturar dois fatos:

(i) Há o mesmo número de subconjuntos em classes de somas de restos diferentes de 0;

(ii) Há dois a subconjuntos a mais com somas divisíveis por p.

Verifiquemos (i). Observe que $\{1; 2; 3; \ldots; 2p\} = \{1; 2; 3; \ldots; p\} \cup \{p+1; p+2; p+3; \ldots; 2p\}$ é a união de dois sistemas de resíduos $\pmod{p}$. Vamos provar que a quantidade de subconjuntos com soma congruente a k (mód. p) é igual à quantidade de subconjuntos com soma congruente a $1 \pmod{p}$. Para obter uma soma congruente a k a partir de uma congruente a 1 basta multiplicarmos tudo por k. No primeiro sistema de resíduos $\{1; 2; 3; \ldots; p\}$ tomamos o resto da divisão do produto por p (exceto se o resto for zero; nesse caso, tomamos p) e no segundo sistema de resíduos tomamos o resto da divisão do produto por p e somamos p (exceto no caso de resto zero, no qual tomamos $2p$). Por exemplo, para $p = 3$ e $k = 2$ fazemos as associações (as barras verticais separam os dois sistemas de resíduos)

$$\begin{aligned}
\{1; 2|4\} &\mapsto \{2; 1|5\} \\
\{1; 3|6\} &\mapsto \{2; 3|6\} \\
\{1|4; 5\} &\mapsto \{2|5; 4\} \\
\{2; 3|5\} &\mapsto \{1; 3|4\} \\
\{2|5; 6\} &\mapsto \{1|4; 6\} \\
\{3|4; 6\} &\mapsto \{3|5; 6\}
\end{aligned}$$

É claro que se $k = 0$ isso não dá certo. Mas veja que a associação é inversível: para obter uma soma congruente a 1 a partir de uma soma congruente a k, basta multiplicar tudo por k^{-1} (por isso p tem que ser primo: todo número $k \not\equiv 0 \pmod{p}$ admite inverso) e fazer a mesma redução dentro de seu respectivo sistema de resíduos. Assim, (i) está demonstrado.

E quanto a (ii)? Já vimos que multiplicar um mesmo número não adianta. Assim, que tal somarmos um mesmo número aos elementos de um subconjunto? Somar a todos os elementos não adianta muito, já que há p elementos em cada subconjunto e somar p vezes qualquer coisa é a mesma coisa que somar 0 (pelo menos, $\bmod p$). Mas podemos escolher somente alguns elementos. Que tal só os elementos do primeiro sistema de resíduos? Se partirmos de um conjunto com soma congruente a zero, com m elementos no primeiro sistema de resíduos e queremos um de soma congruente a k, devemos somar $k \cdot m^{-1}$ a cada elemento desse sistema de resíduos e reduzir a soma para esse sistema. Mas isso só é possível quando m é inversível, o que exclui os conjuntos $\{1; 2; \ldots; p\}$ e $\{p+1; p+2; \ldots; 2p\}$. Note que essa operação é também inversível (para voltar é só subtrair $k \cdot m^{-1}$ de cada elemento do primeiro sistema de resíduos. Veja como fica para $p = 3$, $k = 1$:

$$\begin{aligned}
\{1; 2|6\} &\mapsto \{3; 1|6\} \ (m = 2)\\
\{1; 3|5\} &\mapsto \{3; 2|5\} \ (m = 2)\\
\{1|5; 6\} &\mapsto \{2|5; 6\} \ (m = 1)\\
\{2; 3|4\} &\mapsto \{1; 2|4\} \ (m = 2)\\
\{2|4; 6\} &\mapsto \{3|4; 6\} \ (m = 1)\\
\{3|4; 5\} &\mapsto \{1|4; 5\} \ (m = 1)
\end{aligned}$$

Logo, como o total de subconjuntos com p elementos é $\binom{2p}{p}$, o total desejado é

$$a + 2 = \frac{1}{p}\left[\binom{2p}{p} - 2\right] + 2$$

2.2. Solução 2: Utilizando a Álgebra: Funções Geratrizes

Se você estudou binômio de Newton, deve saber que se n é um inteiro não negativo,

$$(1+x)^n = \sum_{k=1}^{n} \binom{n}{k} x^k = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n$$

Podemos demonstrar isso com um argumento combinatório: observe que

$$(1+x)^n = \underbrace{(1+x) \cdot (1+x) \cdot \ldots \cdot (1+x)}_{n \text{ vezes}}$$

Cada termo de $(1+x)^n$ é o produto de n termos, um de cada fator $1 + x$ acima. Assim, uma parcela x^k em $(1 + x)^n$ é obtido escolhendo-se k termos x, sendo os demais $n - k$ iguais a 1. Logo o número de parcelas x^k é igual ao número de maneiras de escolhermos k dentre n fatores, ou seja, $\binom{n}{k}$. Assim, juntando todos as parcelas, obtemos

$$(1+x)^n = \sum_{k=1}^{n} \binom{n}{k} x^k = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n$$

Às vezes, fazemos o contrário. Para provar ou obter algum resultado combinatório podemos fazer uso de expressões algébricas como o exemplo acima (de certo modo, você também pode supor que o binômio de Newton é verdadeiro – a demonstração pode ser por indução – e *demonstrar* que o número de subconjuntos de k elementos de um conjunto de n elementos é $\binom{n}{k}$).

Tais expressões algébricas são conhecidas como *funções geratrizes*. As funções geratrizes utilizam uma ou mais variáveis para denotar elementos combinatórios. Isso vai ficar mais claro nesse exemplo.

A variável z será um "marcador" dos elementos 1, 2, ..., $2p$ (no nosso exemplo inicial, a variável x denota a presença de um elemento em um subconjunto). Observe que analisamos o produto de termos no nosso exemplo inicial. Considerando que $z^m \cdot z^n = z^{m+n}$ (somamos expoentes e estamos interessados na soma de elementos!), a parcela z^k deve representar o elemento $k \in \{1; 2; 3; \ldots; 2p\}$. Assim, poderíamos considerar a função geratriz

$$f(z) = (1+z)(1+z^2)(1+z^3)\cdots(1+z^{2p})$$

Mas veja que só estamos interessados em subconjuntos com p elementos. Assim, precisamos controlar o número de elementos na nossa função geratriz. Introduzimos, então, uma nova variável y, que marca a presença do elemento no subconjunto:

$$f(y,z) = (1+yz)(1+yz^2)(1+yz^3)\cdots(1+yz^{2p})$$

Cada termo $y^k z^s$ deve ser interpretado como um subconjunto de k elementos (k termos yz^j foram incluídos no subconjunto) e cuja soma dos elementos é s (ao multiplicar os k termos yz^j os expoentes são somados).

Assim, como queremos saber quantos subconjuntos de p elementos têm soma de seus elementos divisível por p, devemos calcular a soma dos termos $y^p z^{pt}$, sendo t inteiro.

Uma das vantagens de utilizar funções geratrizes é ter a Álgebra a seu favor. Por exemplo, podemos substituir z por $\zeta_p \neq 1$, uma raiz complexa p-ésima da unidade, e utilizar o fato de que $\zeta_p^p = 1$ e

$$(y-1)(y-\zeta_p)(y-\zeta_p^2)(y-\zeta_p^3)\cdots(y-\zeta_p^{p-1}) = y^p - 1$$

Os termos $y^p z^{pt}$ serão iguais a $y^p \zeta_p^{pt} = y^p(\zeta_p^p)^t = y^p$ e os termos $y^p z^{pt+r}$, a $y^p \zeta_p^{pt+r} = y^p(\zeta_p^p)^t \zeta_p^r = y^p \zeta_p^r$. Assim, devemos procurar os termos sem ζ_p.

Logo, observando que $1/\zeta_p^j = \zeta_p^{p-j}$ e p é primo ímpar,

$$\begin{aligned}
f(y,\zeta_p) &= (1+y\zeta_p)(1+y\zeta_p^2)\cdots(1+y\zeta_p^p)\cdot \\
&\quad (1+y\zeta_p^{p+1})(1+y\zeta_p^{p+2})\cdots(1+y\zeta_p^{2p}) \\
&= [(1+y\zeta_p)(1+y\zeta_p^2)\cdots(1+y)]^2 \\
&= \left[\frac{(y+\zeta_p^{p-1})(y+\zeta_p^{p-2})\cdots(y+1)}{\zeta_p\cdot\zeta_p^2\cdots\zeta_p^{p-1}}\right]^2 \\
&= \left[\frac{(-1)^p(-y-\zeta_p^{p-1})(-y-\zeta_p^{p-2})\cdots(-y-1)}{\zeta_p^{1+2+\cdots+p-1}}\right]^2 \\
&= \left[\frac{(-1)^p((-y)^p-1)}{\zeta_p^{p(p-1)/2}}\right]^2 \\
&= [y^p+1]^2 = y^{2p} + 2y^p + 1
\end{aligned}$$

Isso quer dizer que há somente 2 subconjuntos? Claramente não, visto que $\{1;2;3;\ldots;p\}$, $\{p+1;p+2;p+3;\ldots;2p\}$ e $\{2;3;4;\ldots;p+1\}$ são três subconjuntos distintos, com p elementos, cujas somas dos elementos ($p(p+1)/2$, $p(3p+1)/2$ e $p(p+3)/2$, respectivamente) são divisíveis por p. O que aconteceu de errado, então? Calma, para tudo há alguma explicação! Veja que

$$\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + 1 = 0$$

e pode ter acontecido de aparecer algo do tipo

$$ay^p\zeta_p^{p-1} + ay^p\zeta_p^{p-2} + \cdots + ay^p = ay^p(\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + 1) = 0$$

De fato, como vimos na solução anterior, os subconjuntos com somas que deixam resto 1, 2, 3, …, $p-1$ são em mesma quantidade. Logo o termo em y^p em $f(y,z)$ é

$$[y^p]f(y,z) = az^{p-1} + az^{p-2} + \cdots + az + b$$

Mas observe que se substituirmos z por ζ_p obtemos 2. Assim,

$$\begin{aligned}
a\zeta_p^{p-1} + a\zeta_p^{p-2} + \cdots + a\zeta_p + b = 2 &\iff a(\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + \zeta_p) + b = 2 \\
&\iff a(-1) + b = 2 \iff b = a + 2
\end{aligned}$$

Logo, como o total de subconjuntos com p elementos é $\binom{2p}{p}$, $a(p-1)+a+2 = \binom{2p}{p} \iff a = \frac{1}{p}\left[\binom{2p}{p} - 2\right]$, de modo que o total desejado é

$$a + 2 = \frac{1}{p}\left[\binom{2p}{p} - 2\right] + 2$$

Para mais sobre funções geratrizes (e belos resultados sobre partições!), veja a referência [4].

3. O método probabilístico

Nem sempre precisamos construir algo para demonstrar sua existência. Podemos fazer isso provando que a probabilidade de ocorrer essa existência é maior que 0 (quando o espaço amostral é finito, isso basta para demonstrar que algo existe).

O chamado *método probabilístico* foi popularizado na Combinatória pelo grande matemático e "resolvedor de problemas" Paul Erdős.

Exemplo 3.1.

Um torneio de tênis com n participantes (onde todos jogam uma única vez contra todos) tem a propriedade S_k se, para todo conjunto X de k participantes do torneio, existe um participante não pertencente a X que venceu todos os participantes de X. Mostre que para cada k existe um torneio com a propriedade S_k.

Resolução

Estimaremos a probabilidade $P(n)$ de um torneio com n participantes **não** ter a propriedade S_k e mostraremos que existe n tal que $P(n) < 1$ (de modo que a probabilidade de o torneio ter S_k é $1 - P(n) > 0$).

Tomemos um torneio em que a probabilidade de cada tenista vencer cada jogo é $1/2$. Fixemos um conjunto X com k participantes. Este conjunto "estraga" o torneio se todos os $n-k$ demais participantes perde de pelo um participante de X. A probabilidade de isso acontecer é $(1 - (\frac{1}{2})^k)^{n-k}$ (por quê?). Como existem $\binom{n}{k}$ conjuntos X's, a probabilidade de um ou mais deles "estragar" o torneio é menor ou igual a $\binom{n}{k}(1 - (\frac{1}{2})^k)^{n-k}$ (ou um estraga ou outro estraga ou...). Logo

$$P(n) < \binom{n}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k} \iff 1 - P(n) > 1 - \binom{n}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k}$$

Deste modo, basta

$$1 - \binom{n}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k} > 0 \iff \binom{n}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k} < 1$$

Seja $f(m) = \binom{m}{k}(1 - (\frac{1}{2})^k)^{m-k}$. Temos

$$\frac{f(m+1)}{f(m)} = \left(1 - \left(\frac{1}{2}\right)^k\right) \cdot \frac{m+1}{m+1-k} = \left(1 - \left(\frac{1}{2}\right)^k\right) \cdot \frac{1}{1 - \frac{k}{m+1}}$$

Como

$$\left(1 - \left(\frac{1}{2}\right)^k\right) \cdot \frac{1}{1 - \frac{k}{m+1}} < 1 \iff m > k \cdot 2^k - 1,$$

então $\frac{f(m+1)}{f(m)} < 1$ para $m > k \cdot 2^k - 1$, o que implica

$$f(m) < a \cdot c^m, \text{ onde } a = \frac{f(k \cdot 2^k - 1)}{c^{k \cdot 2^k - 1}}$$

Assim, sendo a e c constantes com $0 < c < 1$, e c^m arbitrariamente próximo de 0 quando m é suficientemente grande, temos que existe n tal que $f(n) < 1$. ∎

4. Referências Bibliográficas

Os emails foram retirados, na íntegra, da lista de discussão da OBM.

[1] Carlos Shine, Aplicações de Planos Projetivos em Teoria dos Números e Combinatória. Artigo da Revista Eureka! 15.

[2] Timothy Gowers, Two Cultures Of Mathematics.

[3] Albrecht Beutelspacher e Ute Rosenbaum, Projective Geometry.

[4] Eduardo Tengan, Séries Formais. Artigo da Revista Eureka! 11.

[5] Carlos Shine, Probabilidade Aplicada à Teoria dos Grafos. Aula ministrada durante a Semana Olímpica 2001, Salvador.