Universidade de São Paulo
Escola de Artes, Ciências e Humanidades

ACH2013 – Matemática Discreta – 2º sem. 2024
Professor: José Ricardo G. Mendonça

2ª Lista de Exercícios – Quantificadores e Estratégias de Demonstração – 7 out. 2024

Logic, logic, logic. Logic is the beginning of wisdom, Valeris, not the end.
Dr. Spock, in *Star Trek VI: The Undiscovered Country* (1992)

Problemas

I. Funções proposicionais e quantificadores

1. Seja $A = \{1,2,3,4,5\}$. Determine o valor verdade das seguintes proposições:

$$(a)\ (\exists x \in A)\,(x+3=10); \qquad (b)\ (\forall x \in A)\,(x+3<10);$$

$$(c)\ (\exists x \in A)\,(x+3\leqslant 5); \qquad (d)\ (\forall x \in A)\,(x+3<7).$$

2. Seja $A = \{1,2,3\}$. Determine o valor verdade das seguintes proposições:

   (*a*) $(\exists x \in A)\,(\forall y \in A)\,(x^2 < y+1)$;

   (*b*) $(\forall x \in A)\,(\exists y \in A)\,(x^2+y^2<12)$;

   (*c*) $(\forall x \in A)\,(\forall y \in A)\,(x^2+y^2<12)$.

3. Estabeleça a negação das seguintes proposições, onde P e Q são duas funções proposicionais bem definidas quaisquer:

   (*a*) $(\exists x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,P(x,y)$;

   (*b*) $(\forall x \in \mathbb{R})\,(\forall y \in \mathbb{R})\,P(x,y)$;

   (*c*) $(\exists y \in \mathbb{R})\,(\exists x \in \mathbb{R})\,(\forall z \in \mathbb{R})(P(x,y) \wedge Q(x,z))$.

4. Estabeleça a negação das seguintes proposições:

   (*a*) Todos os estudantes de SI da EACH são do sexo masculino;

   (*b*) Alguns estudantes de GPP da EACH têm 25 anos ou mais;

   (*c*) Todos os estudantes da EACH moram na ZL.

5. Descreva em palavras, determine o valor verdade e estabeleça as negações das seguintes proposições:

   (*a*) $(\forall a \in \mathbb{Z})\,(\exists b \in \mathbb{Z})\,(a < b)$;

   (*b*) $(\exists b \in \mathbb{Z})\,(\forall a \in \mathbb{Z})\,(a < b)$.

6. Descreva as seguintes proposições usando quantificadores:

   (*a*) Existem pelo menos três números inteiros distintos que satisfazem a propriedade P;

   (*b*) Existem no máximo três números inteiros distintos que satisfazem a propriedade P.

7. A definição de convergência de uma sequência $(x_n)_{n\in\mathbb{Z}}$ de números reais para um limite x, normalmente denotada por $\lim x_n = x$ ou, abreviadamente, $x_n \to x$, é a seguinte: "para todo número real positivo ε, existe um número inteiro N tal que para todo número inteiro $n > N$ temos que x_n difere de x por menos do que ε". Escreva essa definição usando os devidos quantificadores e proposições.

II. Estratégias de demonstração

1. O ***princípio do pombal*** é um teorema simples que no entanto possui enorme utilidade em toda a matemática. Seu enunciado é o seguinte:[(a)]

   Teorema*: Sejam n e k dois números naturais. Se tentarmos distribuir $n > k$ objetos em k urnas, pelo menos uma das urnas conterá mais de um objeto.*

   Demonstre o princípio do pombal por contraposição.

2. Mostre que se a soma dos dígitos de um número $n \in \mathbb{N}$ qualquer é divisível por 9 então n é divisível por 9 e vice-versa. Notação: se um número n é divisível pelo número d escrevemos $d \,|\, n$, que se lê "d divide n".

3. Para um dado $n \in \mathbb{Z}$, mostre (*a*) de forma direta e (*b*) por contraposição que se n^2 é par, então n é par. Qual das duas demonstrações lhe parece mais objetiva e compreensível?

4. Mostre que todo número primo $p > 3$ é da forma $3k-1$ ou $3k+1$ para algum $k \in \mathbb{N}$.

5. Diga onde está o erro na seguinte demonstração da afirmativa $1+2+\cdots+2^n = 2^{n+1}$: "A propriedade é trivialmente válida para $n = 1$. Suponhamos que ela seja válida para algum $n > 1$, ou seja, que $1+2+\cdots+2^n = 2^{n+1}$. Então $1+2+\cdots+2^n+2^{n+1} = 2^{n+1}+2^{n+1} = 2\cdot 2^{n+1} = 2^{n+2}$, QED."

[(a)] A formulação do princípio do pombal costuma ser atribuída ao matemático alemão Peter Gustav Lejeune Dirichlet (1805–1859) por volta de 1842, embora haja evidências de que o princípio fosse conhecido anteriormente. Dirichlet se referia ao princípio do pombal como *Schubfachprinzip*, ou "princípio da gaveta", em alemão.

6. Prove ou disprove (e neste caso, se for possível corrija) as seguintes proposições:

   (*a*) $\forall n \in \mathbb{N}$, se n é ímpar então $n^2 + 4n$ é ímpar;

   (*b*) $\forall r \in \mathbb{R}$, se r^2 é irracional então r é irracional;

   (*c*) $\forall n \in \mathbb{N}$, $n^5 < 5^n$;

   (*d*) $\forall r \in (-1, \infty)$, $(1+r)^n \geqslant 1 + nr$ (desigualdade de Bernoulli). Porque podemos dizer que essa desigualdade é trivial para $r > 0$?

7. Estabeleça os seguintes resultados usando o princípio de indução finita:[(b)]

   (*a*) $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}(n+1)(2n+1)$ para todo $n \geqslant 1$;

   (*b*) $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$ para todo $n \geqslant 1$. Essa identidade quase milagrosa é conhecida como identidade de Nicômaco de Gerasa (*ca.* 60 – *ca.* 120);

   (*c*) Dados $n \geqslant 2$ números $a_1, \ldots, a_n \in \mathbb{R}$ quaisquer, não todos nulos,

$$\frac{a_1 + a_2 + \cdots + a_n}{1 + a_1 + a_2 + \cdots + a_n} = \frac{a_1}{1 + a_1} + \frac{a_2}{(1 + a_1)(1 + a_1 + a_2)} + \cdots + \frac{a_n}{(1 + a_1 + a_2 + \cdots + a_{n-1})(1 + a_1 + a_2 + \cdots + a_n)}.$$

8. Mostre por indução matemática (ou qualquer outra maneira) que os seguintes resultados de divisibilidade valem para todo $n \in \mathbb{N}$:

   (*a*) $3^n - 1$ é divisível por 2;

   (*b*) $5^n - 2^n$ é divisível por 3;

   (*c*) $2^n + 3^n$ é divisível por 5 se e somente se n é ímpar;

   (*d*) A soma dos cubos de três números inteiros consecutivos é divisível por 9.

9. Mostre que para todo conjunto de $n \geqslant 1$ funções diferenciáveis $f_1(x), \ldots, f_n(x)$ vale

$$\frac{(f_1(x) \cdots f_n(x))'}{f_1(x) \cdots f_n(x)} = \frac{f_1'(x)}{f_1(x)} + \cdots + \frac{f_n'(x)}{f_n(x)}.$$

10. Existem inúmeras demonstrações de que $\sqrt{2}$ é um número irracional. Uma delas consiste em reparar que o último dígito não-nulo de um número inteiro ao quadrado escrito na base 3 deve ser 1, de maneira que a equação $a^2 = 2b^2$ com $a, b \in \mathbb{N}^*$ é impossível. Formalize esse argumento como um lema e um teorema e dê as suas respectivas demonstrações.

[(b)] Uma exposição didática e erudita do princípio da indução finita e do papel das analogias no raciocício matemático é dada por G. Pólya (1887–1985) em *Mathematics and Plausible Reasoning, Volume I: Induction and Analogy in Mathematics* (Princeton, NJ: Princeton University Press, 1954).

11. Números naturais $p \geqslant 2$ que são divisíveis somente por 1 e por eles mesmos são chamados de números primos—por exemplo, 2, 3, 5, 7, 11 são números primos. O ***teorema fundamental da aritmética*** estabelece que todo número natural $n \geqslant 2$ ou é primo ou pode ser fatorado em um produto de número primos.

    (*a*) Tente provar o teorema fundamental da aritmética por indução finita comum;

    (*b*) Prove o teorema fundamental da aritmética usando indução finita forte (também conhecida como indução finita completa).

12. Suponha que n linhas retas são traçadas no plano de tal forma que nenhuma delas é paralela a nenhuma outra e que três linhas diferentes nunca se encontram em um único ponto. Mostre que as linhas dividem o plano em $\frac{1}{2}(n^2+n+2)$ regiões diferentes.

13. Usando indução matemática em n, mostre que se p é um número primo, então $n^p - n$ é divisível por p. Dicas: (*i*) resolva primeiro explicitamente os casos de $p = 2$ e $p = 3$ e (*ii*) use o teorema binomial para o caso de p qualquer. Esse resultado é conhecido como *pequeno teorema de Fermat*,[(c)] estabelecido mas não demonstrado por Pierre de Fermat (1601–1665) em 1640 em uma correspondência.[(d)] Em notação moderna, escrevemos o resultado acima como $n^p \equiv n \pmod{p}$ ou $n^{p-1} \equiv 1 \pmod{p}$, que significam que o resto da divisão de n^p por p vale n ou, equivalentemente, que o resto da divisão de $n^p - n$ por p é nulo, de acordo com o enunciado de nosso problema. Resultados elementares de divisibilidade como esse são muito importantes em técnicas modernas de criptografia, conforme veremos mais adiante em nossa disciplina.

    Existe uma generalização do pequeno teorema de Fermat devida a Leonhard Euler (1707–1783) que estabelece que $n^{\varphi(k)} \equiv 1 \pmod{k}$, onde agora basta que n e k sejam primos entre si, isto é, que $\text{mdc}(n,k) = 1$, e $\varphi(k)$ é a *função totiente de Euler*, que conta o número de inteiros menores que k relativamente primos a k — por exemplo, $\varphi(12) = 4$, enquanto $\varphi(30) = 8$ — verifique. Esses resultados elementares de divisibilidade são muito importantes em técnicas modernas de criptografia.

III. O princípio da inclusão-exclusão

Nos problemas a seguir usamos a notação $\overline{A} = \{x\colon x \notin A\}$ para o conjunto complementar $\Omega \setminus A$, onde $A \setminus B = \{x\colon x \in A,\ x \notin B\}$ denota a diferença entre dois conjuntos A e B quaisquer.

1. Um único conjunto A divide o conjunto universo Ω em duas regiões distintas: A e $\overline{A}$. Dois conjuntos particionam o conjunto universo em no máximo quatro regiões distintas.

(c) Não confundir com o *último teorema de Fermat*, que diz que não existem soluções inteiras positivas para $x^n + y^n = z^n$ com $n \geqslant 3$, enunciado por Fermat em 1637 e demonstrado por Andrew J. Wiles (n. 1953) somente em 1995!

(d) P. Tannery e C. Henry (eds.), *Œvres de Fermat*, Tome Deuxième, *Correspondance* (Paris: Gauthier-Villars, 1894), XLIV – Fermat à Frenicle, 18 octobre 1640, pp. 206–212.

(*a*) Explique como três conjuntos podem dividir o conjunto universo em exatamente 6 regiões distintas e desenhe um diagrama de Venn para ilustrar a situação.

(*b*) Qual é o número máximo de regiões que precisariam ser indexadas se usarmos n conjuntos para particionar o conjunto universo?

2. Mostre que um conjunto S de n elementos possui 2^n subconjuntos. Se $0 < m \leqslant n$, quantos subconjuntos de S possuem exatamente m elementos?

3. Seja $|A|$ o número de elementos de um conjunto finito A. Mostre, usando diagramas de Venn, que para dois conjuntos finitos quaisquer A e B vale $|A \cup B| = |A| + |B| - |A \cap B|$.

4. Suponha que A seja um conjunto com 45 elementos, B seja um conjunto com 32 elementos e C seja um conjunto com 20 elementos.

   (*a*) Qual é o número máximo possível de elementos em $A \cup B \cup C$ e como os conjuntos estão relacionados neste caso?

   (*b*) Qual é o número mínimo possível de elementos em $A \cap B \cap C$ e como os conjuntos estão relacionados neste caso?

   (*c*) Qual é o número máximo possível de elementos em $A \cap (B \cup C)$ e como os conjuntos estão relacionados neste caso?

   Ilustre suas respostas usando diagramas de Venn.

5. Encontre uma expressão para $|A \cup B \cup C|$ e $|A \cup B \cup C \cup D|$ para conjuntos A, B, C e D quaisquer.

6. Uma pesquisa (IBOPE, 2015) mostrou que 79% dos brasileiros se consideram religiosos (acima da média mundial, que é de 63%), enquanto outra pesquisa (CNI, 2015) mostrou que 74% deles nunca fizeram compras *online*. Mostre que o percentual de brasileiros que se consideram religiosos e nunca fizeram compras *online* é maior que 50%.

7. Quantos números inteiros $1 \leqslant n \leqslant 100$ são divisíveis por 2 e também por 3 ou 5?

IV. *Divertissement*: O princípio da inclusão-exclusão

Vimos que para dois conjuntos quaisquer A e B vale a relação $|A \cup B| = |A| + |B| - |A \cap B|$. A generalização desse processo de contagem para n conjuntos, $|A_1 \cup \cdots \cup A_n|$, dá origem a um princípio bastante geral e de enorme aplicação conhecido como ***princípio da inclusão-exclusão***, normalmente abreviado por "PIE" (inclusive em inglês). Esse princípio também é conhecido como ***fórmula do crivo***.

O princípio por trás do PIE para contar corretamente o número de elementos em $A_1 \cup \cdots \cup A_n$ consiste em primeiro superestimar grosseiramente o número de elementos na união pela inclusão

indiscriminada de todos os elementos em cada conjunto, em seguida realizar uma correção simples da estimativa pela exclusão dos elementos que não deveriam ter sido incluídos, depois corrigir essa exclusão pela inclusão dos elementos que não deveriam ter sido excluídos e assim por diante, incluindo e excluindo alternadamente elementos até que na contagem final restem somente os elementos que deveriam ser contados uma única vez. Uma das características mais evidentes de resultados obtidos através do PIE é a presença de somas de termos com sinais alternados.

O teorema a seguir estabelece rigorosamente uma das formas elementares do PIE.

Teorema (Princípio da inclusão-exclusão)**.** *Suponha que temos N objetos e que cada objeto pode possuir ou não uma ou mais das propriedades $a_1, \ldots, a_n$. Denotando o número de objetos com as k propriedades $a_{i_1}, \ldots, a_{i_k}$ por $N(a_{i_1}, \ldots, a_{i_k})$, $1 \leqslant k \leqslant n$, o número de objetos que não possuem qualquer das propriedades $a_1, \ldots, a_n$ é dado por*

$$N - \sum_{i_1} N(a_{i_1}) + \sum_{i_1 < i_2} N(a_{i_1}, a_{i_2}) - \cdots + (-1)^k \sum_{i_1 < \cdots < i_k} N(a_{i_1}, \ldots, a_{i_k}) + \cdots + (-1)^n N(a_1, \ldots, a_n), \tag{1}$$

onde cada índice i_k nos somatórios assume todos os possíveis valores $1, \ldots, n$.

Demonstração. Para demonstrar o PIE na forma acima, basta verificar quantas vezes um objeto qualquer é contado pela expressão (1). Se um objeto não possui qualquer das propriedades, ele é contado uma única vez no termo N em (1) e não contribui para os termos restantes. Um objeto que possui somente uma das propriedades, por sua vez, é contado uma vez em N e uma vez em $\sum_{i_1} N(a_{i_1})$ e, portanto, contribui com $1 - 1 = 0$ para a soma. Já um objeto que possui exatamente $m \geqslant 2$ propriedades é contado uma vez no termo N, m vezes no termo $\sum_{i_1} N(a_{i_1})$, $\binom{m}{2}$ vezes no termo $\sum_{i_1 < i_2} N(a_{i_1}, a_{i_2})$ e assim sucessivamente, isto é, ele é contado $\binom{m}{k}$ vezes em cada termo $\sum_{i_1 < \cdots < i_k} N(a_{i_1}, \ldots, a_{i_k})$, $0 \leqslant k \leqslant m$. A contribuição total desse objeto para a soma vale, portanto,

$$1 - m + \binom{m}{2} - \cdots + (-1)^m \binom{m}{m} = \sum_{k=0}^{m} (-1)^k \binom{m}{k} = (-1+1)^m = 0, \tag{2}$$

pelo teorema binomial.[(e)] Dessa forma, a expressão (1) conta somente os objetos que não possuem qualquer das propriedades $a_1, \ldots, a_n$, como queríamos demonstrar. □

Observação. Se truncarmos a expressão (1) após um termo negativo (respectivamente, positivo), obtemos uma cota inferior (respectivamente, superior) para o número de objetos que não possuem qualquer das propriedades $a_1, \ldots, a_n$. Isso significa que cada termo negativo da soma corrige

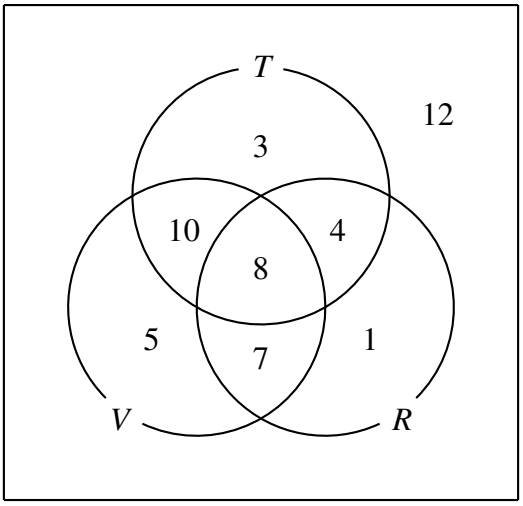
[(e)] O teorema binomial de Newton estabelece que $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$, onde $\binom{n}{k} = n!/k!(n-k)!$ é o coeficiente binomial usual. Colocando $x = -1$ e $y = 1$ nesta expressão obtemos a identidade empregada na equação (2).

um excesso de contagem e cada termo positivo corrige uma deficiência de contagem até aquele ponto.

Exemplo. Vamos dar um exemplo de aplicação do PIE nessa forma. Seja uma coleção de 50 pedras semipreciosas das quais 25 são translúcidas (T), 30 são vermelhas (V), 20 são redondas (R), 18 são translúcidas e vermelhas (T,V), 12 são translúcidas e redondas (T,R), 15 são vermelhas e redondas (V,R) e 8 são translúcidas, vermelhas e redondas (T,V,R). Quantas pedras não são nem translúcidas, nem vermelhas, nem redondas? Uma aplicação direta do PIE fornece

$$\begin{aligned} N_0 &= N - N(T) - N(V) - N(R) + N(T,V) + N(T,R) + N(V,R) - N(T,V,R) \\ &= 50 - 25 - 30 - 20 + 18 + 12 + 15 - 8 = 12. \end{aligned} \tag{3}$$

Outra maneira de resolver esse problema simples seria desenhar o diagrama de Venn dos conjuntos T, V e R e suas interseções, conforme a figura abaixo. Esse dispositivo visual, no entanto, só é prático quando o número de subconjuntos envolvidos no cálculo é pequeno, no máximo 4 ou 5.



Solução do exemplo em termos de diagramas de Venn. Como a soma dos números que aparecem em cada subconjunto disjunto do diagrama vale 38, temos $50 - 38 = 12$ pedras que não pertencem a qualquer das categorias T, V ou R ou suas combinações.

Como o diagrama de Venn empregado no exemplo acima sugere, podemos interpretar o PIE em termos conjuntistas da seguinte forma. Suponha que $A_1, \ldots, A_r$ sejam subconjuntos de um conjunto Ω tais que $A_i = \{x \in \Omega \colon x \text{ possui a propriedade } a_i\}$. Quantos elementos não possuem qualquer das propriedades a_i? Esses são os elementos que estão em $\overline{A}_1 \cap \cdots \cap \overline{A}_r$. Seguindo a receita do PIE, para contá-los tomamos todos os elementos de Ω e subtraímos os elementos que estão em pelo menos um A_i, adicionamos aqueles que estão em pelo menos dois A_i, subtraímos aqueles que aparecem em pelo menos três A_i e assim por diante, e daí ficamos com

$$\left|\overline{A}_1 \cap \cdots \cap \overline{A}_r\right| = |\Omega| - \sum_{i_1} |A_{i_1}| + \sum_{i_1 < i_2} |A_{i_1} \cap A_{i_2}| - \cdots + (-1)^r |A_1 \cap \cdots \cap A_r|. \tag{4}$$

Observação. A expressão acima pode ser escrita de maneira mais compacta como

$$\left|\overline{A}_1 \cap \cdots \cap \overline{A}_r\right| = \sum_{J \subseteq [n]} (-1)^{|J|} \left|A_J\right|, \tag{5}$$

onde $[n]$ é uma notação usual em matemática discreta para o conjunto $\{1,\ldots,n\}$, $J \subseteq [n]$ denota todos os 2^n subconjuntos de $[n]$ e $A_J = \bigcap_{j\in J} A_j$, com a convenção de que $A_\varnothing = \Omega$.

A fórmula do PIE talvez mais conhecida, principalmente em contextos elementares, é aquela usada para calcular $|A_1 \cup \cdots \cup A_r|$, isto é, para determinar o número de objetos que possuem pelo menos uma das propriedades $a_1,\ldots,a_r$. Como, por definição de conjunto complementar, $\Omega = (A_1 \cup \cdots \cup A_r) \cup (\overline{A_1 \cup \cdots \cup A_r})$ e pela lei de DeMorgan $\overline{A_1 \cup \cdots \cup A_r} = \overline{A}_1 \cap \cdots \cap \overline{A}_r$, encontramos que $|A_1 \cup \cdots \cup A_r| = |\Omega| - \left|\overline{A}_1 \cap \cdots \cap \overline{A}_r\right|$ e daí, pela equação (4),

$$|A_1 \cup \cdots \cup A_r| = \sum_{i_1} |A_{i_1}| - \sum_{i_1<i_2} |A_{i_1} \cap A_{i_2}| + \cdots + (-1)^{r-1} |A_1 \cap \cdots \cap A_r|, \tag{6}$$

que generaliza a expressão $|A \cup B| = |A| + |B| - |A \cap B|$ para um número arbitrário de conjuntos.

Uma forma simbólica para o PIE

Podemos obter a fórmula do PIE através de um método conhecido como ***método simbólico***. Dados N objetos que podem possuir ou não uma ou mais das propriedades $a_1,\ldots,a_r$ e denotando o número de objetos com as $k \leqslant r$ propriedades $a_{i_1},\ldots,a_{i_k}$ por $N(a_{i_1}\cdots a_{i_k})$, podemos denotar simbolicamente o número de objetos que não possuem qualquer das propriedades $a_1,\ldots,a_r$ por

$$N_0 = N(a_1' \cdots a_r') = N((1-a_1)\cdots(1-a_r)), \tag{7}$$

onde a_i significa "possui a propriedade i" e $a_i' = 1 - a_i$ significa "não possui a propriedade i". Expandindo o produto $(1-a_1)\cdots(1-a_r)$ encontramos

$$N_0 = N(a_1' \cdots a_r') = N(1 - a_1 - \cdots - a_r + a_1a_2 + \cdots + a_{r-1}a_r - \cdots + (-1)^r a_1 \cdots a_r), \tag{8}$$

e atuando linearmente com o "operador contagem" N sobre a soma ficamos com

$$N_0 = N - N(a_1) - \cdots - N(a_r) + N(a_1a_2) + \cdots + N(a_{r-1}a_r) - \cdots + (-1)^r N(a_1 \cdots a_r), \tag{9}$$

onde colocamos $N(1) = N$. Essa é exatamente a mesma expressão (1) que encontramos inicialmente para o PIE. Algumas dessas expressões, assim como diversas extensões e exemplos de aplicação, foram primeiramente obtidas nessa forma pelo matemático norte-americano Hassler Whitney (1907–1989) no início dos anos 1930 (Whitney, 1932). Riordan (2002) oferece uma exposição detalhada.

Uma das vantagens do método simbólico é que podemos considerar o número de objetos que possuem as propriedades $a_{i_1},\cdots,a_{i_p}$ e não possuem as propriedades $a_{j_1},\cdots,a_{j_q}$, com $p+q=r$, de maneira relativamente trivial: basta considerar

$$N(a_{i_1}\cdots a_{i_p} a_{j_1}' \cdots a_{j_q}') = N(a_{i_1}\cdots a_{i_p}(1-a_{j_1})\cdots(1-a_{j_q})). \tag{10}$$

Por exemplo, se queremos calcular o número de objetos com as propriedades a_1 e a_3 e sem as propriedades a_2 e a_4 calculamos

$$N(a_1a_2'a_3a_4') = N(a_1(1-a_2)a_3(1-a_4)) = N(a_1a_3) - N(a_1a_2a_3) - N(a_1a_3a_4) + N(a_1a_2a_3a_4). \tag{11}$$

Uma vez obtida a expressão desejada, calculamos os termos $N(a_{i_1}\cdots a_{i_p})$ como $\left|A_{i_1}\cap\cdots\cap A_{i_p}\right|$.

Outra vantagem do método simbólico é que ele permite obter uma grande variedade de funções geratrizes, que podem ser manipuladas formalmente (somadas, compostas, derivadas, expandidas em séries *etc*.) e terem o significado combinatorial de seus termos recuperado ao final.

O crivo de Eratóstenes

Eratóstenes (276–194 a.C.) foi um dos bibliotecários da famosa Biblioteca de Alexandria e é lembrado principalmente pela sua medição da circunferência da Terra e pela invenção do crivo numérico que leva seu nome. O ***crivo de Eratóstenes***, descrito pela primeira vez na obra do obscuro matemático grego Nicomedes (280–210 a.C.), consiste de um dispositivo prático para encontrar todos os números primos p no intervalo $2 \leqslant p \leqslant n$ pela eliminação recursiva de todos os números compostos no intervalo de tal forma que os números que sobrevivem ao crivo são todos primos. O crivo de Eratóstenes foi posteriormente aperfeiçoado de muitas maneiras diferentes, levando à introdução de diversas funções aritméticas – por exemplo, a ***função totiente de Euler***, que exploramos a seguir – e a métodos sofisticados conhecidos como ***métodos de crivo*** amplamente empregados em teoria dos números e suas aplicações.[(f)]

O teorema a seguir estabelece a expressão matemática para o crivo de Eratóstenes; sua demonstração envolve a aplicação do PIE.

Teorema (Crivo de Eratóstenes)**.** *O número $\pi(n)$ de números primos entre 2 e n é dado por*

$$\pi(n) = (n-1+k) - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_ip_j} \right\rfloor - \cdots + (-1)^k \left\lfloor \frac{n}{p_1\cdots p_k} \right\rfloor, \tag{12}$$

onde $p_1,\ldots,p_k$ são os números primos entre 2 e $\sqrt{n}$ e $\lfloor x\rfloor$ denota o maior inteiro menor ou igual a x.

Para demonstrar esse teorema vamos primeiro estabelecer um importante lema auxiliar.

Lema. *Para encontrar os números primos p no intervalo $2 \leqslant p \leqslant n$, basta eliminar todos os múltiplos dos números primos entre 2 e $\sqrt{n}$. Os números restantes no intervalo após a eliminação são todos primos.*

[(f)] Veja, por exemplo, Gérald Tenenbaum e Michel M. France, *The Prime Numbers and Their Distribution* (Providence, RI: American Mathematical Society, 2000).

Demonstração. Se n é um número composto $n = pq$ com $2 \leqslant p \leqslant q$, então $p^2 \leqslant pq = n$, de onde segue que $p \leqslant \sqrt{n}$. Isso nos permite concluir que para encontrar todos os números primos $2 \leqslant p \leqslant n$ basta eliminar os múltiplos dos números primos entre 2 e $\sqrt{n}$, já que nenhum número maior que $\sqrt{n}$ e menor ou igual a n que sobra depois da eliminação possui fator primo menor ou igual a $\sqrt{n}$ tampouco pode ser produto de dois números maiores que $\sqrt{n}$. □

Observação. Os números primos obtidos pelo procedimento do lema acima não correspondem a todos os números primos no intervalo $2, \ldots, n$ porque o procedimento, exatamente como descrito, em princípio elimina também os números primos p no intervalo $2 \leqslant p \leqslant \sqrt{n}$. Essa observação é relevante na obtenção da fórmula (14) para o crivo de Eratóstenes.

Na demonstração do lema aparecem números $n = pq$ com p e q primos. Números desse tipo, dados pelo produto de dois números primos muito grandes de aproximadamente mesma quantidade (atualmente, centenas) de dígitos, são empregados em criptografia porque são mais difíceis de fatorar, fornecendo maior segurança criptográfica.[(g)]

De posse do lema acima podemos demonstrar a fórmula para o crivo de Eratóstenes como uma simples aplicação do PIE.

Demonstração. Sejam $p_1, \ldots, p_k$ os números primos entre 2 e $\sqrt{n}$ e seja $N(p_1 \cdots p_j) = \lfloor n/p_1 \cdots p_j \rfloor$ o número de múltiplos de $p_1 \cdots p_j$, $j = 1, \ldots, k$, entre 2 e n. Pelo lema e pelo PIE, o número de inteiros entre 2 e n que não são múltiplos de nenhum primo $p_1, \ldots, p_k$ vale

$$(n-1) - \sum_i N(p_i) + \sum_{i<j} N(p_i p_j) - \cdots + (-1)^k N(p_1 \cdots p_k), \tag{13}$$

onde o termo $(n-1)$ corresponde à quantidade de números inteiros entre 2 e n. O número dado por (13), no entanto, ainda não corresponde à quantidade de números primos entre 2 e n, pois falta incluir na contagem os k números primos $p_1, \ldots, p_k$ eles próprios. Assim, o número $\pi(n)$ de números primos entre 2 e n é dado, finalmente, por

$$\pi(n) = (n-1+k) - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \cdots + (-1)^k \left\lfloor \frac{n}{p_1 \cdots p_k} \right\rfloor, \tag{14}$$

que é a expressão matemática para o crivo de Eratóstenes. □

Exemplo. Seja $n = 170$. Neste caso, os números primos entre 2 e $\sqrt{170}$ são 2, 3, 5, 7, 11 e 13. Para empregar a fórmula (14), podemos considerar somente os termos até $N(3,5,11)$, porque qualquer combinação dos primos 2, 3, 5, 7, 11 e 13 envolvendo números maiores que

[(g)] Veja, por exemplo, Abramo Hefez, *Aritmética*, 2a. ed. (Rio de Janeiro, RJ: Sociedade Brasileira de Matemática, 2016) e Manfred R. Schroeder, *Number Theory in Science and Communication – With Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity*, 5th ed. (Berlin: Springer, 2009).

$p_i p_j p_k = 3 \cdot 5 \cdot 11$ ou mais de 3 fatores (por exemplo, $p_i p_j p_k p_\ell = 2 \cdot 3 \cdot 5 \cdot 7$) será maior que 170. O resto é simples aritmética: temos $N(2) = \lfloor 170/2 \rfloor = 85$, $N(3) = \lfloor 170/3 \rfloor = 56$, ..., $N(2,3) = \lfloor 170/6 \rfloor = 28$ e assim por diante até $N(3,5,11) = \lfloor 170/165 \rfloor = 1$. Juntando tudo obtemos

$$\begin{aligned} \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor &= 85+56+34+24+15+13 = 227, \\ \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor &= 28+17+12+7+6+11+8+5+4+4+3+2+2+1+1 = 111, \\ \sum_{i<j<k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor &= 5+4+2+2+2+1+1+1+1+1 = 20, \end{aligned} \tag{15}$$

de onde concluímos, pelo crivo de Eratóstenes (14), que existem $\pi(170) = (170-1+6) - 227 + 111 - 20 = 39$ números primos entre 2 e 170. O leitor pode querer verificar quais são esses primos.

$\star$ — $\star$ — $\star$

O dominó da indução finita: se você mostrar que a proposição vale para $n = 1$ (derrubar o primeiro dominó) e que se ela vale para $n = k$ (a hipótese de indução) então vale para $n = k+1$ também (o passo de indução), então a proposição vale para todo n (todo dominó em queda atinge o próximo e todos eles caem).