Capítulo 16

Respostas aos exercícios

1 Vamos contar!

1.1 Uma festa

1.1. $7 \cdot 6 \cdot \ldots \cdot 2 \cdot 1 = 5040$.

1.2. Carl: $15 \cdot 2^3 = 120$. Diane: $15 \cdot 3 \cdot 2 \cdot 1 = 90$.

1.3. Bob: $9 \cdot 7 \cdot 5 \cdot 3 = 945$. Carl: $945 \cdot 2^5 = 30240$. Diane: $945 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 113400$.

1.2 Conjuntos

1.4. (a) todas as casas em uma rua; (b) uma equipe olímpica; (c) classe de '99; (d) todas as árvores em uma floresta; (e) o conjunto dos números racionais; (f) um círculo no plano.

1.5. (a) soldados; (b) pessoas; (c) livros; (d) animais.

1.6. (a) todas as cartas em uma pilha; (b) todas as cartas de espada em uma pilha; (c) uma pilha de cartas suíças; (d) inteiros não-negativos com no máximo dois dígitos; (e) inteiros não-negativos com exatamente dois dígitos; (f) habitantes de Budapest, Hungria.

1.7. Alice, e o conjunto cujo único elemento é o número 1.

1.8. Não.

1.9. $\emptyset, \{0\}, \{1\}, \{3\}, \{0,1\}, \{0,3\}, \{1,3\}, \{0,1,3\}$. 8 subconjuntos.

1.10. mulheres; pessoas na festa; estudantes de Yale.

1.11. $\{a\}, \{a,c\}, \{a,d\}, \{a,e\}, \{a,c,d\}, \{a,c,e\}, \{a,d,e\}, \{a,c,d,e\}$.

1.12. $\mathbb{Z}$ or $\mathbb{Z}_+$. O menor é $\{0,1,3,4,5\}$.

1.13. (a) $\{a,b,c,d,e\}$. (b) A operação de união é associativa. (c) A união de qualquer conjunto de conjuntos consiste daqueles elementos que são elementos de pelo menos um dos conjuntos.

1.14. A união de um conjunto de conjuntos $\{A_1, A_2, \ldots, A_k\}$ é o menor conjunto contendo cada A_i como um subconjunto.

1.15. $6, 9, 10, 14$.

1.16. A cardinalidade da união é no mínimo a maior entre n e m e no máximo $n + m$.

1.17. (a) $\{1, 3\}$; (b) $\emptyset$; (c) $\{2\}$.

1.18. A cardinalidade da interseção é no máximo o mínimo entre n e m.

1.19. A comutatividade (1.2) é obvia. Para mostrar que $(A \cap B) \cap C = A \cap (B \cap C)$, basta verificar que ambos os lados consistem daqueles elementos que pertencem a todos os três A, B e C. A prova da outra identidade em (1.3) é semelhante. Finalmente, podemos provar (1.4) de modo inteiramente análogo à prova de (1.1).

1.20. Os elementos comuns entre A e B são contados duas vezes em ambos os lados; os elementos em A ou B, mas não ambos, são contados uma vez em ambos os lados.

1.21. (a) O conjunto dos inteiros pares negativos e inteiros ímpares positivos. (b) B.

1.3 O número de of subconjuntos

1.22. (a) Potências de 2. (b) $2^n - 1$. (c) conjuntos não contendo o último elemento.

1.23. 2^{n-1}.

1.24. Divida todos os subconjuntos em pares, de modo que cada par seja diferente de outro somente no seu último elemento. Cada par contém um subconjunto par e um ímpar, portanto seus números são os mesmos.

1.25. (a) $2 \cdot 10^n - 1$; (b) $2 \cdot (10^n - 10^{n-1})$.

1.26. 101.

1.27. $1 + \lfloor n \lg 2 \rfloor$.

1.5 Seqüências

1.28. As árvores têm 9 e 12 folhas, respectivamente.

1.29. $5 \cdot 4 \cdot 3 = 60$.

1.30. 3^{13}.

1.31. $6 \cdot 6 = 36$.

1.32. 12^{20}.

1.33. $(2^{20})^{12}$.

1.6 Permutações

1.34. $n!$.

1.35. (a) $7 \cdot 5 \cdot 3 \cdot 1 = 105$. (b) $(2n - 1) \cdot (2n - 3) \cdot \ldots \cdot 3 \cdot 1$.

1.7 O número de subconjuntos ordenados

1.36. (Não achamos que você poderia realmente desenhar toda a árvore; ela tem quase 10^{20} folhas. Ela tem 11 níveis de nós.)

1.37. (a) $100!$. (b) $90!$. (c) $100!/90! = 100 \cdot 99 \cdot \ldots \cdot 91$.

1.38. $\frac{n!}{(n-k)!} = n(n-1) \cdot (n-k+1)$.

1.39. Em um caso, a repetição não é permitida, enquanto que no outro caso, ela é permitida.

1.8 O número de subconjuntos de um dado tamanho

1.40. Apertos de mão; loteria; mãos de cartas em bridge.

1.41. Veja o Triângulo de Pascal no Capítulo 3.

1.42. $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = \binom{n}{n-1} = n$.

1.43. Uma prova algébrica de (1.7) é imediata. Em (1.8), o lado direito conta k-subconjuntos de um conjunto de n-elementos contando separadamente aqueles que contêm um dado elemento e aqueles que não.

1.44. Uma prova algébrica é fácil. Uma interpretação combinatória: n^2 é o número de todos os pares ordenados (a, b) com $a, b \in \{1, 2, \ldots, n\}$. $\binom{n}{2}$ é o número de pares ordenados (a, b) entre esses com $a < b$ (por que?). Para contar os pares ordenados remanescentes (a, b) (aqueles com $a \geq b$), adicione 1 a seu primeiro elemento. Então obtemos um par (a', b) com $1 \leq a', b \leq n + 1$, $a' > b$, e vice-versa, todo par desse é obtido dessa maneira. Daí o número desses pares é $\binom{n+1}{2}$.

1.45. Novamente, uma prova algébrica é fácil. Uma interpretação combinatória: Podemos escolher um conjunto de k-elementos primeiro escolhendo um elemento (n possibilidades) e então escolher um subconjunto de $(k-1)$-elementos dos $n-1$ elementos remanescentes ($\binom{n-1}{k-1}$ possibilidades). Mas obtemos cada subconjunto de k-elementos exatamente k vezes (dependendo de qual dos seus elementos foi escolhido primeiro), portanto temos que dividir o resultado por k.

1.46. Ambos os lados contam o número de maneiras de dividir divide um conjunto de a-elementos em três conjuntos com $a - b$, $b - c$, e c elementos.

2 Ferramentas combinatórias

2.1 Indução

2.1. Um dos dois: n ou $n + 1$, é par, portanto o produto $n(n + 1)$ é par. Por indução: verdadeiro para $n = 1$; se $n > 1$ então $n(n + 1) = (n - 1)n + 2n$, e $n(n - 1)$ é par pela hipótese de indução, $2n$ é par, e a soma de dois números pares é par.

2.1. Verdadeiro para $n = 1$. Se $n > 1$ então

$$1 + 2 + \ldots + n = (1 + 2 + \ldots + (n - 1)) + n = \frac{(n - 1)n}{2} + n = \frac{n(n + 1)}{2}.$$

2.2. A pessoa mais jovem contará n apertos de mãos. O sétimo mais velho contará 6 apertos de mãos. Portanto eles contarão $1 + 2 + \ldots + n$ apertos de mãos. Já sabemos que existem $n(n + 1)/2$ apertos de mãos.

2.3. Calcule a área retângulo de duas maneiras diferentes.

2.4. Por indução sobre n. Verdadeiro para $n = 2$. Para $n > 2$, temos

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + (n - 1) \cdot n = \frac{(n - 2) \cdot (n - 1) \cdot n}{3} + (n - 1) \cdot n$$

$$= \frac{(n-1)\cdot n\cdot (n+1)}{3}.$$

2.5. Se n for par, então $1+n = 2+(n-1) = ... = \left(\frac{n}{2}-1\right)+\frac{n}{2} = n+1$, portanto a soma é $\frac{\frac{n}{2}(n+1)=n(n+1)}{2}$. Se n for ímpar então temos que adicionar o termo do meio separadamente.

2.6. Se n for par, então $1+(2n-1) = 3+(2n-3) = \ldots = (n-1)+(n+1) = 2n$, portanto a soma é $\frac{n}{2}(2n) = n^2$. Novamente, se n for ímpar a solução é similar, mas temos que adicionar o termo do meio separadamente.

2.7. Por indução. Verdadeiro para $n = 1$. Se $n > 1$ então

$$1^2+2^2+\ldots+(n-1)^2 = (1^2+2^2+\ldots+(n-1)^2)+n^2 = \frac{(n-1)n(2n-1)}{6}+n^2$$

$$= \frac{n(n+1)(2n+1)}{6}.$$

2.8. Por indução. Verdadeiro para $n = 1$. Se $n > 1$ então

$$2^0+2^1+2^2+\ldots+2^{n-1} = (2^0+2^1+\ldots+2^{n-2})+2^{n-1}$$

$$= (2^{n-1}-1)+2^{n-1} = 2^n-1.$$

2.9. (Cadeias) Verdadeiro para $n = 1$. Se $n > 1$ então para obter uma cadeia de comprimento n podemos começar com uma cadeia de comprimento $n-1$ (essa pode ser escolhida de k^{n-1} maneiras pela hipótese da indução) e concatenar um elemento (esse pode ser escolhido de k maneiras). Portanto obtemos $k^{n-1}\cdot k = k^n$.
(Permutações) Verdadeiro para $n = 1$. Para assentar n pessoas, podemos começar assentando a mais velha (isso pode ser feito de n maneiras) e então assentar o restante (isso pode ser feito de $(n-1)!$ maneiras pela hipótese da indução). Obtemos $n\cdot(n-1)! = n!$.

2.10. Verdadeiro se $n = 1$. Seja $n > 1$. O número de apertos de mão n pessoas é o número de apertos de mão dados pela pessoa mais velha (isso é $n-1$) mais o número de apertos de mão entre as $n-1$ pessoas restantes (o que é $(n-1)(n-2)/2$ pela hipótese da indução). Obtemos $(n-1)+(n-1)(n-2)/2 = n(n-1)/2$ apertos de mão.

2.11. Não verificamos o caso base $n = 1$.

2.12. A prova usa a afirmação de que existem pelo menos quatro linhas. Mas apenas verificou $n = 1, 2$ como casos base. A asserção é falsa para $n = 3$ e para todo valor de n depois desse.

2.2 Comparando e estimando números

2.13. (a) o lado esquerdo conta todos os subconjuntos de um n-conjunto, o lado direito conta apenas os subconjuntos de 3-elementos. (b) $2^n/n^2 > \binom{n}{3}/n^2 = (n-1)(n-2)/(6n)$, que fica arbitrariamente grande.

2.14. Comece a indução com $n = 4$: $4! = 24 > 16 = 2^4$. Se a desigualdade vale para n, então $(n+1)! = (n+1)n! > (n+1)2^n > 2\cdot 2^n = 2^{n+1}$.

2.3 Inclusão-exclusão

2.15. $18 + 23 + 21 + 17 - 9 - 7 - 6 - 12 - 9 - 12 + 4 + 3 + 5 + 7 - 3 = 40$.

2.4 Casas de pombo

2.16. Se cada uma das caixas gigantes contém no máximo 20 nova-iorquinos, então 500.000 boxes contém no máximo $20 \cdot 500,000 = 10,000,000$ nova-iorquinos, o que é uma contradição.

3 Coeficientes binomiais e o Triângulo de Pascal

3.1 O Teorema Binomial

3.1.
$(x+y)^{n+1}$

$$\begin{aligned}
&= (x+y)^n(x+y) \\
&= \left(x^n + \binom{n}{1}x^{n-1}y + \ldots + \binom{n}{n-1}xy^n + \binom{n}{n}y^n\right)(x+y) \\
&= x^n(x+y) + \binom{n}{1}x^{n-1}y(x+y) + \ldots \\
&\quad + \binom{n}{n-1}xy^{n-1}(x+y) + \binom{n}{n}y^n(x+y) \\
&= (x^{n+1} + x^n y) + \binom{n}{1}(x^n y + x^{n-1}y^2) + \ldots \\
&\quad + \binom{n}{n-1}(x^2y^{n-1} + xy^n) + \binom{n}{n}(xy^n + y^{n+1}) \\
&= x^{n+1} + \left(1 + \binom{n}{1}\right)x^n y + \left(\binom{n}{1} + \binom{n}{2}\right)x^{n-1}y^2 + \ldots \\
&\quad + \left(\binom{n}{n-1} + \binom{n}{n}\right)xy^n + y^{n+1} \\
&= x^{n+1} + \binom{n+1}{1}x^n y + \binom{n+1}{2}x^{n-1}y^2 + \ldots + \binom{n+1}{n}xy^n + y^{n+1}.
\end{aligned}$$

3.2. (a) $(1-1)^n = 0$. (b) Devido a $\binom{n}{k} = \binom{n}{n-k}$.

3.3. A identidade diz que *o número de subconjuntos de um conjunto de n-elementos com um número par de elementos é o mesmo que o número de subconjuntos com um número ímpar de elementos.* Podemos estabelecer uma bijeção entre subconjuntos pares e ímpares da seguinte maneira: se um subconjunto contém 1, remova-o do subconjunto; caso contrário, adicione-o ao subconjunto.

3.2 Distribuindo presentes

3.4.

$$\begin{aligned}&\binom{n}{n_1}\cdot\binom{n-n_1}{n_2}\cdot\ldots\cdot\binom{n-n_1-\ldots-n_{k-1}}{n_k}\\&=\frac{n!}{n_1!(n-n_1)!}\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdots\frac{(n-n_1-\ldots-n_{k-1})!}{n_{k-1}!(n-n_1-\ldots-n_k)!}\\&=\frac{n!}{n_1!n_2!\ldots n_k!},\end{aligned}$$

pois $n-n_1-\ldots-n_{k-1}-n_k=0$.

3.5. (a) $n!$ (distribua posições ao invés de presentes). (b) $n(n-1)\ldots(n-k+1)$ (distribua como "presentes" as primeiras k posições na competição e $n-k$ certificados de participação). (c) $\binom{n}{n_1}$. (d) Assentamento para jogo de xadrez no sentido de Diane (distribua jogadores a tabuleiros).

3.6. (a) $[n=8]\,8!$. (b) $8!\cdot\binom{8}{4}$. (c) $(8!)^2$.

3.3 Anagramas

3.7. $13!/2^3$.

3.8. COMBINATORICS.

3.9. Máximo: qualquer palavra com 13 letras diferentes; mínimo: qualquer palavra com 13 letras idênticas.

3.10. (a) 26^6.
(b) $\binom{26}{4}$ maneiras de escolher as quatro letras que ocorrem; para cada escolha, $\binom{4}{2}$ maneiras de escolher as duas letras que ocorrem duas vezes; para cada escolha, distribuimos 6 posições a essas letras (2 delas recebem 2 posições), isso dá $\frac{6!}{2!2!}$ maneiras. Por conseguinte obtemos $\binom{26}{4}\binom{4}{2}\frac{6!}{2!2!}$. (Existem muitas outras maneiras de se chegar ao mesmo número!)
(c) Número de maneiras de particionar 6 na soma de inteiros positivos:

$$6=6=5+1=4+2=4+1+1=3+3=3+2+1=3+1+1+1$$

$$=2+2+2=2+2+1+1=2+1+1+1+1=1+1+1+1+1+1,$$

o que faz 11 possibilidades.
(d) Esse não é tão difícil nessa forma. Q que queremos dizer é o seguinte: quantas palavras de comprimento n existem tais que nenhuma é um anagrama de uma outra? Isso significa distribuir n pennies a 26 crianças, e portanto a resposta é $\binom{n+25}{25}$.

3.4 Distribuindo dinheiro

3.11. $\binom{n-k-1}{k-1}$.

3.12. $\binom{n+k-1}{\ell+k-1}$.

3.13. $\binom{kp+k-1}{k-1}$.

3.5 Triângulo de Pascal

3.14. Isso é o mesmo que $\binom{n}{k} = \binom{n}{n-k}$.

3.15. $\binom{n}{0} = \binom{n}{n} = 1$ (e.g. pela fórmula geral para os coeficientes binomiais).

3.6 Identidades no Triângulo de Pascal

3.16.

$$\begin{aligned}
&1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} \\
&= 1 + \left[\binom{n-1}{0} + \binom{n-1}{1}\right] + \left[\binom{n-1}{1} + \binom{n-1}{2}\right] + \\
&\quad \ldots + \left[\binom{n-1}{n-2} + \binom{n-1}{n-1}\right] + 1 \\
&= 2\left[\binom{n-1}{0} + \binom{n-1}{1} + \ldots + \binom{n-1}{n-2} + \binom{n-1}{n-1}\right] \\
&= 2 \cdot 2^{n-1} = 2^n.
\end{aligned}$$

3.17. O coeficiente de $x^n y^n$ em

$$\left(\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \ldots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n\right)^2$$

is

$$\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \ldots + \binom{n}{n-1}\binom{n}{1} + \binom{n}{n}\binom{n}{0}.$$

3.18. O lado esquerdo conta todos os subconjuntos de k-elementos de um conjunto de $(n+m)$-elementos distinguindo-os de acordo com quantos elementos eles pegam dos primeiros n.

3.19. Se o maior elemento é j (que é pelo menos $n+1$), então o restante pode ser escolhido de $\binom{j-1}{n}$ maneiras. Se somarmos para todo $j \geq n+1$, obtemos a identidade

$$\binom{n}{n} + \binom{n+1}{n} + \ldots + \binom{n+k}{n} = \binom{n+k+1}{n+1}.$$

Usando o fato de que $\binom{n+i}{n} = \binom{n+i}{i}$, obtemos (3.5).

3.7 Uma visão de águia do Triângulo de Pascal

3.20. $n = 3k + 2$.

3.21. Esse não é fácil. Olhe para a diferença das diferenças:

$$\left(\binom{n}{k+1} - \binom{n}{k}\right) - \left(\binom{n}{k} - \binom{n}{k-1}\right).$$

Desejamos determinar o primeiro valor de k para o qual ela se torna negativa. Podemos dividir a expressão por $\binom{n}{k-1}$ e multiplicar por $k(k+1)$ para obter

$$(n-k+1)(n-k) - 2(n-k+1)(k+1) + k(k+1) \ ? \ 0.$$

Simplificando,

$$4k^2 - 4nk + n^2 - n - 2 \ ? \ 0.$$

Resolvendo para k, obtemos que o lado esquerdo é não-positivo entre as duas raízes:

$$\frac{n}{2} - \frac{1}{2}\sqrt{n+2} \leq k \leq \frac{n}{2} + \frac{1}{2}\sqrt{n+2}.$$

Portanto o primeiro inteiro k para o qual isso é não-positivo é

$$k = \left\lceil \frac{n}{2} - \frac{1}{2}\sqrt{n+2} \right\rceil.$$

3.22. (a) Temos que mostrar que $e^{-t^2/(m-t+1)} \leq e^{-t^2/m} \leq e^{-t^2/(m+t)}$. Isso é imediato usando o fato de que e^x é uma função crescente monotônica.
(b) Tome a razão do limite superior pelo limite inferior:

$$\frac{e^{-t^2/(m+t)}}{e^{-t^2/(m-t+1)}} = e^{t^2/(m-t+1) - t^2/(m+t)}.$$

Aqui o expoente é

$$\frac{t^2}{m-t+1} - \frac{t^2}{m+t} = \frac{(2t-1)t^2}{(m-t+1)(m+t)}.$$

Em nosso caso, isso é $1900/(41*60) \approx .772$, e portanto a razão é $e^0 .772 \approx 2.1468$.

3.23. Por (3.9), temos

$$\binom{2m}{m} \Big/ \binom{2m}{m-t} \geq e^{t^2/(m+t)}.$$

Aqui o expoente é uma função crescente monotônica de t para $t \geq 0$ (para ver isso, escreva-a como $t(1 - \frac{m}{m+t})$, ou tome sua derivada), e portanto de nossa suposição de que $t \geq \sqrt{m \ln C} + \ln C$ segue que

$$\begin{aligned} \frac{t^2}{m+t} &\geq \frac{(\sqrt{m \ln C} + \ln C)^2}{m + \sqrt{m \ln C} + \ln C} = \frac{\ln C(m + 2\sqrt{m \ln C} + \ln C)}{m + \sqrt{m \ln C} + \ln C} \\ &> \ln C, \end{aligned}$$

o que implica que

$$\binom{2m}{m} \Big/ \binom{2m}{m-t} > C.$$

A prova da outra metade é semelhante.

4 Números de Fibonacci

4.1 Exercício de Fibonacci

4.1. Porque usamos os dois elementos anteriores para calcular o próximo.

4.2. F_{n+1}.

4.3. Vamos denotar por S_n o número de subconjuntos bons. Se $n = 1$, então $S_1 = 2$ (o conjunto vazio e o conjunto $\{1\}$. Se $n = 2$, então $\emptyset$, $\{1\}$, $\{2\}$, portanto S_2=3. Para qualquer n se o subconjunto contém n, então ele não pode conter $n-1$, portanto existem S_{n-2} subconjuntos desse tipo, se ele não contém n, então existem S_{n-1} subconjuntos. Portanto temos a mesma fórmula recursiva, portanto $S_n = F_{n+2}$.

4.2 Muitas identidades

4.4. Está claro da recorrência que dois números ímpares são seguidos por um par, e então por dois números ímpares novamente.

4.5. Formulamos o seguinte enunciado aparentemente malvado: *se n é divisível por 5, então F_n também o é; se n tem resto 1 quando dividido por 5, então F_n tem resto 1; se n tem resto 2 quando dividido por 5, então F_n tem resto 1; se n tem resto 3 quando dividido por 5, então F_n tem resto 2; se n tem resto 4 quando dividido por 5, então F_n tem resto 3.* Isso é então facilmente provado por indução sobre n.

4.6. Por indução. Todos eles são verdadeiros para $n = 1$ e $n = 2$. Assuma que $n \geq 3$.

(a) $F_1+F_3+F_5+\ldots+F_{2n-1} = (F_1+F_3+\ldots+F_{2n-3})+F_{2n-1} = F_{2n-2}+F_{2n-1} = F_{2n}$.

(b) $F_0 - F_1 + F_2 - F_3 + \ldots - F_{2n-1} + F_{2n} = (F_0 - F_1 + F_2 - \ldots + F_{2n-2}) + (-F_{2n-1} + F_{2n}) = (F_{2n-3} - 1) + F_{2n-2} = F_{2n-1} - 1$.

(c) $F_0^2 + F_1^2 + F_2^2 + \ldots + F_n^2 = (F_0^2 + F_1^2 + \ldots + F_{n-1}^2) + F_n^2 = F_{n-1}F_n + F_n^2 = F_n(F_{n-1} + F_n) == F_n \cdot F_{n+1}$.

(d) $F_{n-1}F_{n+1} - F_n^2 = F_{n-1}(F_{n-1} + F_n) - F_n^2 = F_{n-1}^2 + F_n(F_{n-1} - F_n) = F_{n-1}^2 - F_nF_{n-2} = -(-1)^{n-1} = (-1)^n$.

4.7. Podemos escrever (4.1) como $F_{n-1} = F_{n+1} - F_n$, e usar isso para calcular F_n para n negativo recursivamente (de trás para frente):

$$\ldots -21,\ 13,\ -8,\ 5,\ -3,\ 2,\ -1,\ 1,\ 0$$

É fácil reconhecer que esses são o mesmo que os números de Fibonacci usuais, exceto que todo segundo tem um sinal negativo. Na fórmula,

$$F_{-n} = (-1)^{n+1}F_n.$$

Isso é agora facilmente provado por indução sobre n. É verdadeiro para $n = 0, 1$, e assumindo que ele é verdadeiro para n e $n-1$, obtemos para $n+1$:

$$F_{-(n+1)} = F_{-(n-1)} - F_{-n} = (-1)^n F_{n-1} - (-1)^{n+1}F_n$$

$$= (-1)^n(F_{n-1} + F_n) = (-1)^n F_{n+1} = (-1)^{n+2}F_{n+1},$$

o que completa a indução.

4.8.

$$F_{n+2} = F_{n+1} + F_n = (F_n + F_{n-1}) + F_n = 2F_n + (F_n - F_{n-2}) = 3F_n - F_{n-2}.$$

Substituindo n por $2n-1$, obtemos a recorrência para números de Fibonacci de índice-ímpar. Usando isso para provar (4.2):

$$\begin{aligned} F_{n+1}^2 + F_n^2 &= (F_n + F_{n-1})^2 + F_n^2 = 2F_n^2 + F_{n-1}^2 + 2F_nF_{n-1} \\ &= 3F_n^2 + 2F_{n-1}^2 - (F_n - F_{n-1})^2 = 3F_n^2 + 2F_{n-1}^2 - F_{n-2}^2 \\ &= 3(F_n^2 + F_{n-1}^2) - (F_{n-1}^2 + F_{n-2}^2) = 3F_{2n-1} - F_{2n-3} \\ &= F_{2n+1}. \end{aligned}$$

4.9. A identidade é

$$\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \ldots + \binom{n-k}{k} = F_{n+1},$$

onde $k = \lfloor n/2 \rfloor$. Prova por indução. Verdadeiro para $n = 0$ e $n = 1$. Seja $n \geq 2$. Assuma que n é ímpar; o caso par é semelhante, somente o último termo abaixo precisa de um tratamento um pouco diferente.

$$\begin{aligned} &\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \ldots + \binom{n-k}{k} \\ &= 1 + \left(\binom{n-2}{0} + \binom{n-2}{1}\right) + \left(\binom{n-3}{1} + \binom{n-3}{2}\right) + \ldots \\ &\quad + \left(\binom{n-k-1}{k-1} + \binom{n-k-1}{k}\right) \\ &= \left(\binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \ldots + \binom{n-k-1}{k}\right) \\ &\quad + \left(\binom{n-2}{0} + \binom{n-3}{1} + \ldots + \binom{n-k-1}{k-1}\right) \\ &= F_n + F_{n-1} = F_{n+1}. \end{aligned}$$

4.10. (4.2) segue tomando-se $a = b = n - 1$. (4.3), segue tomando-se $a = n$, $b = n - 1$.

4.11. Seja $n = km$. Usamos indução sobre m. Para $m = 1$ a asserção é óbvia. Se $m > 1$, então usamos (4.5) com $a = k(m-1)$, $b = k - 1$:

$$F_{ka} = F_{(k-1)a}F_{a-1} + F_{(k-1)a+1}F_a.$$

Pela hipótese da indução, ambos os termos são divisíveis por F_a.

4.12. A "diagonal" é na verdade um paralelogramo muito longo e estreito com área 1. O truque depende do fato de que $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ é muito pequeno comparado a F_n^2.

4.3 Uma fórmula para os números de Fibonacci

4.13. Verdadeiro para $n = 0, 1$. Seja $n \geq 2$. Então pela hipótese da indução,

$$\begin{aligned}
F_n &= F_{n-1} + F_{n-2} \\
&= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right) \\
&\quad + \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\right) \\
&= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}}{2}+1\right) + \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}}{2}+1\right)\right) \\
&= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \left(\frac{1-\sqrt{5}}{2}\right)^{n}\right).
\end{aligned}$$

4.14. Para $n = 1$ e $n = 2$, se requeremos que L_n seja da forma dada, então obtemos

$$L_1 = 1 = a + b, \qquad L_2 = 3 = a\frac{1+\sqrt{5}}{2} + b\frac{1-\sqrt{5}}{2}.$$

Resolvendo para a e b, obtemos

$$a = \frac{1+\sqrt{5}}{2}, \qquad b = \frac{1-\sqrt{5}}{2}.$$

Então

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n,$$

o que segue por indução sobre n tal qual no problema anterior.

4.15. (a) Por exemplo: todo dia Jack compra um sorvete por \$1 ou um sundae gigante por \$2. Existem 4 sabores diferentes de sorvete, mas somente um tipo de sundae. Se ele tem n dólares, de quantas maneiras ele pode gastar o dinheiro?

$$I_n = \frac{1}{2\sqrt{5}}\Big((2+\sqrt{5})^n - (2-\sqrt{5})^n\Big).$$

4.16. A fórmula funciona para $n = 1, 2 \ldots, 10$ mas falha para $n = 11$, quando ela dá 91. Na verdade, ficará mais e mais fora à medida que n cresce. Vimos que

$$F_n \sim \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n = 0.447\ldots \cdot 1.618\ldots^n.$$

Na fórmula de Alice, a rodada tem um menor papel, daí

$$\lceil e^{n/2-1} \rceil \sim e^{n/2-1} = 0.367\ldots 1.648\ldots^n,$$

e portanto a razão entre os números de Alice e os números de Fibonacci correspondentes é

$$\frac{\lceil e^{n/2-1} \rceil}{F_n} \sim \frac{0.367\ldots 1.648\ldots^n}{0.447\ldots} = 0.822\ldots 1.018\ldots^n$$

Como a base da exponencial é maior que 1, isso tende ao infinito à medida que n cresce.

5 Probabilidade combinatória

5.1 Eventos e probabilidades

5.1. A união de dois eventos A e B corresponde a "A ou B", i.e., pelo menos um dos dois A ou B ocorre.

5.2. É a soma de alguma das probabilidades de resultados, e mesmo se somar todas as probabilidades, obtemos somente 1.

5.3. $\mathsf{P}(E) = \frac{1}{2}$, $\mathsf{P}(T) = \frac{1}{3}$.

5.4. As mesmas probabilidades $\mathsf{P}(s)$ são somadas em ambos os lados.

5.5. Toda probabilidade $\mathsf{P}(s)$ com $s \in A \cap B$ é adicionada duas vezes a ambos os lados; toda probabilidade $\mathsf{P}(s)$ com $s \in A \cup B$ porém $s \notin A \cap B$ é adicionada uma vez a ambos os lados.

5.2 Repetição independente de um experimento

5.6. Os pares $(E,T), (O,T), (L,T)$ são independentes. O par (E,O) é exclusivo. Nem o par (E,L) nem o par (O,L) é independente.

5.7. $\mathsf{P}(\emptyset \cap A) = \mathsf{P}(\emptyset) = 0 = \mathsf{P}(\emptyset)\mathsf{P}(A)$. O conjunto S também tem esse propriedade: $\mathsf{P}(S \cap A) = \mathsf{P}(A) = \mathsf{P}(S)\mathsf{P}(A)$.

5.8. $\mathsf{P}(A) = \frac{|S|^{n-1}}{|S|^n} = \frac{1}{|S|}$, $\mathsf{P}(B) = \frac{|S|^{n-1}}{|S|^n} = \frac{1}{|S|}$, $\mathsf{P}(A \cap B) = \frac{|S|^{n-2}}{|S|^n} = \frac{1}{|S|^2} = \mathsf{P}(A)\mathsf{P}(B)$.

5.9. A probabilidade de que sua mãe tenha o mesmo dia de aniversário que você é $1/365$ (aqui assumimos que dias de aniversário são distribuídos igualmente entre todos os números do ano, e ignoramos anos bissextos). Esses eventos são independentes para sua mãe, pai, e cônjuge, portanto a probabilidade de que para uma dada pessoa, todos os três tivessem nascido no seu dia de aniversário é $1/365^3 = 1/48,627,125$. Existem (aproximadamente) 6 bilhões de pessoas no mundo. Vamos dizer 2 bilhões deles são casados: podemos esperar que $2,000,000,000/48,627,125 \approx 41$ deles tenham o mesmo dia de aniversário que sua mãe, pai, e cônjuge.

6 Inteiros, divisores, e primos

6.1 Divisibilidade de inteiros

6.1. $a = a \cdot 1 = (-a) \cdot (-1)$.

6.2. (a) par; (b) ímpar; (c) $a = 0$.

6.3. (a) Se $b = am$ e $c = bn$ então $c = amn$. (b) Se $b = am$ e $c = an$ então $b + c = a(m+n)$ e $b - c = a(m-n)$. (c) Se $b = am$ e $a, b > 0$ então $m > 0$, daí

$m \geq 1$ e portanto $b \geq a$. (d) Trivial se $a = 0$. Assuma $a \neq 0$. Se $b = am$ e $a = bn$ então $a = amn$, logo $mn = 1$. Daí ou $m = n = 1$, ou $m = n = -1$.

6.4. Temos $a = cn$ e $b = cm$, daí $r = b - aq = c(m - nq)$.

6.5. Temos $b = am$, $c = aq + r$ e $c = bt + s$. Donde $s = c - bt = (aq + r) - (am)t = (q - mt)a + r$. Como $0 \leq r < a$, o resto da divisão $s : a$ é r.

6.6. (a) $a^2 - 1 = (a - 1)(a + 1)$. (b) $a^n - 1 = (a - 1)(a^{n-1} + \ldots + a + 1)$.

6.3 Fatoração em primos

6.7. Existe um menor entre os criminosos *positivos* (de fato, em todo conjunto de inteiros positivos), mas um conjunto de inteiros negativos não precisa ter um menor elemento (se ele é infinito).

6.8. Sim, o número 2.

6.9. (a) p ocorre na fatoração prima de ab, portanto ele tem que ocorrer na fatoração prima de a ou na fatoração prima de b.
(b) $p|a(b/a)$, mas $p \nmid a$, portanto, devido a (a), temos que ter $p|(b/a)$.

6.10. Seja $n = p_1 p_2 \ldots p_k$; cada $p_i \geq 2$, donde $n \geq 2^k$.

6.11. Se $r_i = r_j$ então $ia - ja$ é divisível por p. Mas $ia - ja = (i - j)a$ e nem a nem $i - j$ são divisíveis por p. Donde os r_i são todos diferentes. Nenhum deles é 0. A quantidade deles é $p - 1$, portanto todo valor $1, 2, \ldots, p - 1$ tem que ocorrer entre os r_i.

6.12. Para um primo p, a prova é a mesma que para 2. Se n é composto mas não um quadrado, então existe um primo p que ocorre na fatoração prima de n um número ímpar de vezes. Podemos repetir a prova olhando para esse p.

6.13. Fato: Se $\sqrt[k]{n}$ não é um inteiro então ele é irracional. Prova: existe um primo que ocorre na fatoração prima de n, digamos t vezes, onde $k \nmid t$. Se (suposição indireta) $\sqrt[k]{n} = a/b$ então $nb^k = a^k$, e portanto o número de vezes que p ocorre na fatoração prima do lado esquerdo não é divisível por k, enquanto que o número de vezes que ele ocorre na fatoração prima do lado direito é divisível por k. Uma contradição.

6.4 Sobre o conjunto de primos

6.14. Tal qual no tratamento do caso $k = 200$ acima, subtraímos o número de primos até 10^{k-1} do número de primos até 10^k. Pelo Teorema do Número Primo, esse número é cerca de

$$\frac{10^k}{k \ln 10} - \frac{10^{k-1}}{(k-1)\ln 10} = \frac{(9k - 10)10^{k-1}}{k(k-1)\ln 10}$$

Como

$$\frac{9k - 10}{k - 1} = 9 - \frac{1}{k - 1}$$

é muito próximo a 9 se k for grande, obtemos que o número de primos com k dígitos é aproximadamente

$$\frac{9 \cdot 10^{k-1}}{k \ln 10}.$$

Comparando isso com o número total de inteiros positivos com k dígitos, que sabemos que é $10^k - 10^{k-1} = 9 \cdot 10^{k-1}$, obtemos

$$\frac{9 \cdot 10^{k-1}}{k \ln 10 \cdot 9 \cdot 10^{k-1}} = \frac{1}{(\ln 10)k} \approx \frac{1}{2.3k}.$$

6.5 "Pequeno" Teorema de Fermat

6.15. $4 \nmid \binom{4}{2} = 6$. $4 \nmid 2^4 - 2 = 14$.

6.16. (a) Precisamos que cada uma das p cópias rotacionadas de conjunto são diferentes. Suponha que existe uma cópia rotacionada que ocorre a vezes. Então trivialmente qualquer outra cópia rotacionada ocorre a vezes. Mas então $a|p$, portanto temos que ter $a = 1$ ou $a = p$. Se todas as p cópias rotacionadas são a mesma, então trivialmente $k = 0$ ou $k = p$, que foram excluídas. Portanto temos $a = 1$ conforme afirmado. (b) Considere o conjunto de dois vértices opostos de um quadrado. (c) Se cada caixa contém p subconjuntos de tamanho k, o número total de subconjuntos tem que ser divisível por p.

6.17. Considere que cada número tenha p dígitos, adicionando-se zeros na frente se necessário. Obtemos p números de cada número a por deslocamento cíclico. Esses são todos o mesmo quando todos os dígitos de a são o mesmo, mas todos diferentes caso contrário (por que? a suposição de que p é um primo é necessária aqui!). Portanto obtemos $a^p - a$ números que são divididos em classes de tamanho p. Por conseguinte $p|a^p - a$.

6.18. Assuma que $p \nmid a$. Considere o produto $a(2a)(3a)\ldots((p-1)a) = (p-1)!a^{p-1}$. Seja r_i o resto de ia quando dividido por p. Então o produto acima tem o mesmo resto quando dividido por p que o produto $r_1 r_2 \ldots r_{p-1}$. Mas esse produto é justamente $(p-1)!$. Donde p é um divisor de $(p-1)!a^{p-1} - (p-1)! = (p-1)!(a^{p-1} - 1)$. Como p é um primo, ele não é um divisor de $(p-1)!$, e portanto ele é um divisor de $a^{p-1} - 1$.

6.6 O Algoritmo Euclideano

6.19. $\mathrm{mdc}(a, b) \leq a$, mas a é um divisor comum, portanto $\mathrm{mdc}(a, b) = a$.

6.20. (a) Seja $d = \mathrm{mdc}(a, b)$. Então $d|a$ e $d|b$, e portanto $d|b - a$. Por conseguinte d é um divisor comum de a e $b - a$, e portanto $d \leq \mathrm{mdc}(a, b)$. Um argumento semelhante mostra a desigualdade reversa. (b) Por aplicação repetida de (a).

6.21. (a) $\mathrm{mdc}(a/2, b)|(a/2)$ e portanto $\mathrm{mdc}(a/2, b)|a$. Logo $\mathrm{mdc}(a/2, b)$ é um divisor comum de a e b e portanto $\mathrm{mdc}(a/2, b) \leq \mathrm{mdc}(a, b)$. A desigualdade reversa segue de modo similar, usando o fato de que $\mathrm{mdc}(a, b)$ é ímpar, e portanto $\mathrm{mdc}(a, b)|(a/2)$. (b) $\mathrm{mdc}(a/2, b/2)|(a/2)$ e portanto $2\mathrm{mdc}(a/2, b/2)|a$. De modo semelhante, $2\mathrm{mdc}(a/2, b/2)|b$, e portanto $2\mathrm{mdc}(a/2, b/2) \leq \mathrm{mdc}(a, b)$. Reciprocamente, $\mathrm{mdc}(a, b)|a$ e portanto $\frac{1}{2}\mathrm{mdc}(a, b)|a/2$. De modo semelhante, $\frac{1}{2}\mathrm{mdc}(a, b)|b/2$, e portanto $\frac{1}{2}\mathrm{mdc}(a, b) \leq \mathrm{mdc}(a/2, b/2)$.

6.22. Considere cada primo que ocorre em um deles, eleve-o ao maior dos dois expoentes, e multiplique essas potências primas.

6.23. Se a e b são os dois inteiros, e você conhece a fatoração prima de a, então tome os fatores primos de a um por um, divida b por eles repetidamente para determinar o expoente deles na factoração prima de b, eleve-os ao menor dos seus expoentes na fatoração prima de a e b, e multiplique essas potências primas.

6.24. Pelas descrições do mdc e do mmc acima, cada primo ocorre o mesmo número de vezes na fatoração prima de ambos os lados.

6.25. (a) Imediato. (b) Seja $z = \mathrm{mdc}(a, b, c)$, e suponha que $A = a/z$, $B = b/z$, $C = c/z$. Então A, B e C são primos entre si e formam uma tripla pitagórica. Um dos dois A ou B tem que ser ímpar, pois se ambos fossem pares, então C também seria, e portanto eles não seriam primos entre si. Suponha que B seja ímpar. Então A tem que ser par. De fato, o quadrado de um número ímpar dá um resto de 1 quando dividido por 4, portanto se ambos A e B fossem ímpares, então $C^2 = A^2 + B^2$ daria um resto de 2 quando dividido por 4, o que é impossível. Segue que C tem que ser ímpar.
Portanto A é par, e podemos escrevê-lo na forma $A = 2A_0$. Escreva a equação na forma

$$A_0^2 = \frac{C+B}{2}\frac{C-B}{2}.$$

Seja p um número primo qualquer dividindo A_0. Então p tem que dividir ou $(C+B)/2$ ou $(C-B)/2$. Mas p não divide ambos, pois então ele também dividiria a soma $\frac{C+B}{2} + \frac{C-B}{2} = C$ assim como a diferença $\frac{C+B}{2} - \frac{C-B}{2} = B$, contradizendo a suposição de que A, B e C são primos entre si.
O primo p pode ocorrer na decomposição prima de A_0 várias vezes, digamos k vezes. Então na decomposição prima de A_0^2, p ocorre $2k$ vezes. Pelo argumento acima, p tem que ocorrer $2k$ vezes na decomposição prima de um dos dois $(C+B)/2$ e $(C-B)/2$, e de forma alguma na decomposição prima do outro.
Portanto vemos que na decomposição prima de $(C+B)/2$ (e igualmente na decomposição prima de $(C-B)/2$), todo primo ocorre com uma potência par. Isso é o mesmo que dizer que ambos $(C+B)/2$ e $(C-B)/2$ são quadrados: digamos, $(C+B)/2 = x^2$ e $(C-B)/2 = y^2$ para alguns inteiros x e y.
Agora podemos expressar A, B e C em termos de x e y:

$$B = \frac{C+B}{2} - \frac{C-B}{2} = x^2 - y^2, C = \frac{C+B}{2} + \frac{C-B}{2} = x^2 + y^2,$$

$$A = 2A_0 = 2\sqrt{\frac{C+B}{2}\frac{C-B}{2}} = 2xy.$$

Obtemos a, b e c multiplicando A, B e C por z, o que completa a solução.

6.26. $\mathrm{mdc}(a, a+1) = \mathrm{mdc}(a, 1) = \mathrm{mdc}(0, 1) = 1$.

6.27. O resto de F_{n+1} quando dividido por F_n é F_{n-1}. Daí $\mathrm{mdc}(F_{n+1}, F_n) = \mathrm{mdc}(F_n, F_{n-1}) = \ldots = \mathrm{mdc}(F_3, F_2) = 1$. Isso leva $n-1$ passos.

6.28. Por indução sobre k. Verdadeiro se $k = 1$. Suponha que $k > 1$. Seja $b = aq + r$, $1 \leq r < a$. Então o algoritmo euclideano para calcular $\mathrm{mdc}(a, r)$ leva $k-1$ passos, donde $a \geq F_k$ e $r \geq F_{k-1}$ pela hipótese da indução. Mas então $b = aq + r \geq a + r \geq F_k + F_{k-1} = F_{k+1}$.

6.29. (a) Leva 10 passos. (b) Segue de $\mathrm{mdc}(a,b) = \mathrm{mdc}(a-b,b)$. (c) $\mathrm{mdc}(10^{100}-1, 10^{100}-2)$ leva $10^{100}-1$ passos.

6.30. (a) Leva 8 passos. (b) Pelo menos um dos números permanece ímpar o tempo todo. (c) Segue dos exercícios 6.20 e 6.21. (d) O produto dos dois números cai de um fator de dois em uma de quaisquer duas iterações.

6.7 Congruências

6.31. $m = 54321 - 12345 = 41976$.

6.32. Somente (b) está correto.

6.33. $a \equiv b \pmod 0$ deveria significar que existe um inteiro k tal que $a - b = 0 \cdot k$. Isso significa que $a - b = 0$, ou $a = b$. Portanto igualdade pode ser considerada como um caso especial de congruência.

6.34. (a) Tome $a = 2$ e $b = 5$. (b) Se $ac \equiv bc \pmod{mc}$ então $mc|ac - bc$, portanto existe inteiro k tal que $ac - bc = kmc$. Como $c \neq 0$, isso implica que $a - b = km$, e portanto $a \equiv b \pmod m$.

6.35. Primeiro, de $x \equiv y \pmod p$ segue (pela regra da multiplicação) que $x^v \equiv y^v \pmod p$, portanto basta provar que

$$x^u \equiv x^v \pmod p. \tag{16.1}$$

Se $x \equiv 0 \pmod p$, então ambos os lados de (16.1) são divisíveis por p, e a asserção segue. Suponha que $x \not\equiv 0 \pmod p$. Suponha que, digamos, $u < v$. Sabemos que $p - 1|v - u$, portanto podemos escrever $v - u = k(p-1)$ com algum inteiro positivo k. Agora sabemos pelo Pequeno Teorema de Fermat que $x^{p-1} \equiv 1 \pmod p$, donde pela regra da multiplicação de congruências, temos $x^{k(p-1)} \equiv 1 \pmod p$, e pela regra da multiplicação novamente, obtemos $x^v = x^u \cdot x^{k(p-1)} \equiv x^u \pmod p$, o que prova (16.1).

6.8 Números estranhos

6.36. Ter; Sab; Qui; Qua.

6.37. não-$A = 1 \oplus A$; A-ou-$B = A \oplus B \oplus A \cdot B$; A-e-$B = A \cdot B$.

6.38. $2 \cdot 0 \equiv 2 \cdot 3 \pmod 6$ mas $0 \not\equiv 3 \pmod 6$. De maneira mais geral, se $m = ab$ $(a, b > 1)$ é um módulo composto, então $a \cdot 0 \equiv a \cdot b \pmod m$, mas $0 \not\equiv b \pmod m$.

6.39. Começamos com o algoritmo euclideano:

$$\mathrm{mdc}(53, 234527) = \mathrm{mdc}(53, 2) = \mathrm{mdc}(1, 2) = 1.$$

Aqui obtemos 2 como $2 = 234527 - 4425 \cdot 53$, e então 1 como

$$1 = 53 - 26 \cdot 2 = 53 - 26(234527 - 4425 \cdot 53) = 115051 \cdot 53 - 26 \cdot 234527$$

Segue que $1 \equiv 115051 \cdot 53 \pmod{234527}$, e portanto $\overline{1}/\overline{53} = \overline{115051}$.

6.40. $x \equiv 5,\ y \equiv 8 \pmod{11}$.

6.41. (a) Temos $11|x^2 - 2x = x(x-2)$, donde $11|x$ ou $11|x-2$, portanto $x \equiv 0 \pmod{11}$ e $x \equiv 2 \pmod{11}$ são as duas soluções. (b) Igualmente, de $23|x^2 - 4 = (x-2)(x+2)$ obtemos $x \equiv 2 \pmod{23}$ ou $x \equiv -2 \pmod{23}$.

6.9 Teoria dos números e combinatória

6.42. Existem dois inteiros vizinhos k e $k+1$ entre os n números dados (Princípio da Casa de Pombos), que são primos entre si.

6.43. Pelas regras da inclusão-exclusão, temos que subtrair de n o número de múltiplos de p_i (entre 1 e n) para todo p_i; então temos que adicionar o número de múltiplos comuns de p_i e p_j para quaisquer dois primos p_i e p_j; então temos que subtrair o número de múltiplos comuns de p_i, p_j e p_k para quaisquer três primos p_i, p_j e p_k, etc. Tal qual no exemplo númerico, o número de múltiplos de p_i é n/p_i; o número de múltiplos comuns de p_i e p_j é $n/(p_ip_j)$; o número de múltiplos comuns de p_i, p_j e p_k é $n/(p_ip_jp_k)$, etc. Portanto obtemos

$$\phi(n) = n - \frac{n}{p_1} - \ldots - \frac{n}{p_r} + \frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \ldots + \frac{n}{p_{r-1}p_r} - \frac{n}{p_1p_2p_2} - \ldots$$

Isso é igual à expressão em (6.7). De fato, se expandirmos o produto, todo termo surge escolhendo-se "1" ou "$-\frac{1}{p_i}$" de cada fator "$\left(1 - \frac{1}{p_i}\right)$", o que dá um termo da forma

$$(1-)^k \frac{1}{p_{i_1} \cdots p_{i_k}}.$$

Isso é justamente um termo típico na fórmula da inclusão-exclusão acima.

6.44. Nào é difícil chegar à conjectura de que a resposta é n. Para provar isso, considere as frações $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$, e simplifique-as tanto quanto possível. Obtemos frações da forma $\frac{a}{d}$, onde d é um divisor de n, $1 \leq a \leq d$, and $\mathrm{mdc}(a,d) = 1$. Está claro também que obtemos toda fração como essa. O número de tais frações com um dado denominador é $\phi(d)$. Como o número total de frações com as quais começamos é n, isso prova nossa conjectura.

6.45. Para $n = 1$ e 2 a resposta é 1. Suponha que $n > 2$. Se k é um tal inteiro, então $n-k$ também o é. Portanto esses inteiros vêm em pares totalizando n (temos que acrescentar que $n/2$ não está entre esses números). Existem $\phi(n)/2$ tais pares, portanto a resposta é $n\phi(n)/2$.

6.46. A prova é semelhante à solução do exercício 6.18.
Sejam $s_1, \ldots, s_k$ os números entre 1 e b primos em relação a b; portanto $k = \phi(b)$. Seja r_i o resto de s_ia quando dividido por p. Temos $\mathrm{mdc}(b, r_i) = 1$, pois se existisse um primo p dividindo ambos b e r_i, então p também dividiria s_ia, o que é impossível, pois ambos s_i e a são primos em relação a b. Segundo, $r_1, r_2, \ldots, r_k$ são diferentes, pois $r_i = r_j$ significaria que $b|s_ia - s_ja = (s_i - s_j)a$; como $\mathrm{mdc}(a,b) = 1$, isso implicaria que $b|s_i - s_j$, o que é claramente impossível. Donde segue que $r_1, r_2, \ldots, r_k$ são justamente os números $s_1, s_2, \ldots, s_k$, em ordem diferente.
Considere o produto $(s_1a)(s_2a)\ldots(s_ka)$. Por um lado podemos escrever isso como

$$(s_1a)(s_2a)\ldots(s_ka) = (s_1s_2\ldots s_k)a^k,$$

por outro lado,

$$(s_1a)(s_2a)\ldots(s_ka) \equiv r_1r_2\ldots r_k = s_1s_2\ldots s_k. \pmod b.$$

Comparando,

$$(s_1s_2\ldots s_k)a^k \equiv s_1s_2\ldots s_k \pmod b,$$

ou

$$b \mid (s_1s_2\ldots s_k)(a^k-1)$$

Como $s_1s_2\ldots s_k$ é primo em relação a b, isso implica que $b|a^k-1$ tal qual afirmado.

6.10 Como testar se um número é um primo?

6.47. Por indução sobre k. Verdadeiro se $k=1$. Seja $n=2m+a$, onde a é 0 ou 1. Então m tem $k-1$ bits, portanto por indução, podemos computar 2^m usando no máximo $2(k-1)$ multiplicações. Agora $2^n=(2^m)^2$ se $a=0$ e $2^n=(2^m)^2\cdot 2$ se $a=1$.

6.48. Se $3|a$ então claramente $3|a^{561}-a$. Se $3\nmid a$, então $3|a^2-1$ por Fermat, donde $3|(a^2)^{280}-1=a^{560}-1$. Igualmente, se $11\nmid a$, então $11|a^{10}-1$ e portanto $11|(a^{10})^{56}-1=a^{560}-1$. Finalmente, se $17\nmid a$, então $17|a^{16}-1$ e portanto $17|(a^{16})^{35}-1=a^{560}-1$.

7 Grafos

7.1 Graus pares e ímpares

7.1. Existem 2 grafos sobre 2 nós, 8 grafos sobre 3 nós (mas somente quatro "essencialmente diferentes"), 64 grafos sobre 4 nós (mas somente 11 "essencialmente diferentes").

7.2. (a) Não; o número de graus ímpares tem que ser par. (b) Não; nó com grau 5 tem que estar conectado a todos os outros nós, portanto não podemos ter um nó com grau 0. (c) 12 (mas eles são todos "essencialmente o mesmo"). (d) $9\cdot 7\cdot 5\cdot 3\cdot 1=945$ (mas novamente eles são todos "essencialmente o mesmo").

7.3. Esse grafo, o *grafo completo* tem $\binom{n}{2}$ arestas se ele tiver n nós.

7.4. No grafo (a), o número de arestas é 17, os graus são $9,5,3,3,2,3,1,3,2,3$. No grafo (b), o número de arestas é 31, os graus são $9,5,7,5,8,3,9,5,7,4$.

7.5. $\binom{10}{2}=45$.

7.6. $2^{\binom{20}{2}}=2^{190}$.

7.7. *Todo grafo tem dois nós com o mesmo grau.* Como cada grau está entre 0 e $n-1$, se todos os graus fossem diferentes então eles seriam $0,1,2,3,\ldots n-1$ (em alguma ordem). Mas o nó com grau $n-1$ tem que estar conectado a todos os outros, em particular ao nó com grau degree 0, o que é impossível.

7.2 Caminhos, ciclos, e conectividade

7.8. Existem 4 caminhos, 6 ciclos e 1 grafo completo.

7.9. O grafo vazio sobre n nós tem 2^n subgrafos. O triângulo tem 18 subgrafos.

7.10. O caminho de comprimento 3 e o ciclo de comprimento 5 são os únicos exemplos. (O complemento de um caminho ou ciclo mais longo tem arestas demais.)

7.11. Sim, a prova permanece válida.

7.12. (a) Remova qualquer aresta de um caminho. (b) Considere dois nós u e v. O grafo original contém um caminho conectando-os. Se esse caminho não passa por e, então ele continua sendo um caminho após e ser removida. Se ele passa por e, então seja $e = xy$, e assuma que o caminho atinge x primeiro (quando percorrido de u para v). Então após e ser removida, existe um caminho no grafo remanescente de u para x, e também de x para y (o restante do ciclo), portanto existe um de u para y. Mas existe também um de y para v, portanto existe também um caminho de u para v.

7.13. (a) Considere uma caminhada mais curta de u para v; se essa passa por quaisquer nós mais de uma vez, a parte dela entre duas passadas por esse nó pode ser removida, para torná-la mais curta. (b) Os dois caminhos juntos formam uma caminhada de a para c.

7.14. Seja w um nó comum de H_1 e H_2. Se você deseja um caminho entre nós u e v em H, então podemos tomar um caminho de u para w, seguido por um caminho de w para v, para obter uma caminhada de u para w.

7.15. Ambos os grafos são conexos.

7.16. A união dessa aresta e um desses componentes formaria um grafo conexo que é estritamente maior que o componente, contradizendo a definição de um componente.

7.17. Se u e v estão no mesmo componente conexo, então esse componente, e portanto G também, contém um caminho conectando-os. Reciprocamente, se existe um caminho P em G conectando u e v, então esse caminho é um subgrafo conexo, e um subgrafo conexo maximal contendo P é um componente conexo contendo u e v.

7.18. Assuma que o grafo não seja conexo e suponha que um seu componente conexo H tenha k nós. Então H tem no máximo $\binom{k}{2}$ arestas. O resto do grafo tem no máximo $\binom{n-k}{2}$ arestas. Então o número de arestas é no máximo

$$\binom{k}{2} + \binom{n-k}{2} = \binom{n-1}{2} - (k-1)(n-k-1) \leq \binom{n-1}{2}.$$

7.13 Caminhadas eulerianas e ciclos hamiltonianos

7.19. O grafo superior esquerdo não tem uma caminhada euleriana. O grafo inferior esquerdo tem uma caminhada euleriana aberta. Os dois grafos à direita têm caminhadas eulerianas fechadas.

7.20. Todo nó com um grau ímpar tem que ser uma extremidade de uma das duas caminhadas, portanto uma condição necessária é que o número de nós com grau ímpar é no máximo quatro. Mostramos que essa condição é também suficiente. Sabemos que o número de nós com grau ímpar é par. Se esse número é 0 ou 2, então existe uma única caminhada euleriana (e podemos tomar qualquer nó individualmente como a outra caminhada).

Suponha que esse número seja quatro. Acrescente uma nova aresta, conectando dois desses nós com grau ímpar. Então existem apenas dois nós com grau ím par restantes, portanto o grafo tem uma caminhada euleriana. Remover a aresta divide essa caminhada em duas, que juntas usam toda aresta exatamente uma vez.

7.21. O primeiro grafo sim; o segundo não.

8 Árvores

8.1 Como definir uma árvore?

8.1. Se G é uma árvore então ele não contém ciclos (por definição), mas acrescentar qualquer nova aresta cria um ciclo (com o caminho na árvore conectando as extremidades da nova aresta). Reciprocamente, se um grafo não tem ciclos mas acrescentar qualquer aresta cria um ciclo, então ele é conexo (dois nós u e v são conectados por uma aresta, ou então adicionar uma resta conectando-os cria um ciclo, que contém um caminho entre u e v no grafo anterior), e por conseguinte ele é uma árvore.

8.2. Se u e v estão no mesmo componente conexo, então a nova aresta uv forma um ciclo com o caminho conectando u e v no grafo anterior. Se a junção de u e v por meio de uma nova aresta cria um ciclo, então o resto desse ciclo é caminho entre u e v, e portanto u e v estão no mesmo componente.

8.3. Assuma que G seja uma árvore. Então existe pelo menos um caminho entre dois nós, por conectividade. Mas não pode haver dois caminhos, pois então obteríamos um ciclo (encontre o nó v quando os dois caminhos se separam, e siga o segundo caminho até ele tocar o primeiro caminho novamente; siga o primeiro caminho de volta a v, para obter um ciclo).
Reciprocamente, assuma que exista um único caminho entre cada par de nós. Então o grafo é conexo (pois existe um caminho) e não pode conter um ciclo (pois dois nós no ciclo teriam pelo menos dois caminhos conectando-os).

8.2 Como crescer uma árvore?

8.4. Comece o caminho de um nó de grau 1.

8.5. Qualquer aresta tem apenas um senhor, pois se houvesse dois, eles teriam que começar de extremidades diferentes, e eles teriam então duas maneiras de chegar ao Rei: ou continuando como eles começaram, ou esperando pelo outro e caminhando juntos. Da mesma forma, uma aresta sem senhor teria que levar a duas maneiras diferentes de caminhar.

8.6. Comece em qualquer nó v. Se um dos ramos nesse nó contém mais que metade de todos os nós, mova-se ao longo da aresta levando a esse ramo. Repita. Você nunca voltará porque isso significaria que existe uma aresta cuja remoção resulta em dois componentes conexos, ambos contendo mais que metade dos nós. Você nunca retornará a um nó já visto porque o grafo é uma árvore. Por conseguinte você é obrigado a parar num nó tal que cada ramo nesse nó contém no máximo metade de todos nos nós.

8.3 Como contar árvores?

8.7. O número de árvores não-rotuladas sobre $2, 3, 4, 5$ nós é $1, 1, 2, 3$. Elas dão origem a um total de $1, 3, 16, 125$ árvores rotuladas.

8.8. Existem n estrelas e $n!/2$ caminhos sobre n nós.

8.4 Como armazenar uma árvore?

8.9. O primeiro é o código-pai de um caminho; o terceiro é o código-pai de uma estrela. Os outros dois não são códigos-pai árvores.

8.10. Esse é o número de códigos-pai possíveis.

8.11. Defina um grafo sobre $\{1, \ldots, n\}$ conectando todos os pares de nós na mesma coluna. Se o fizermos de-trás-para-frente, começando com a última coluna, obtemos um procedimento de crescimento de uma árvore adicionando um novo nó e uma aresta conectando-o a um nó antigo.

8.12. (a) codifica um caminho; (b) codifica uma estrela; (c) não codifica qualquer árvore (existem mais 0's que 1's entre os primeiros 5 elementos, o que é impossível no código planar de qualquer árvore).

9 Encontrando o ótimo

9.1 Encontrando a melhor árvore

9.1. Seja H uma árvore ótima e suponha que G seja a árvore construída pelo governo pessimista. Olhe para o primeiro passo quando uma aresta $e = uv$ de H é eliminada. Removendo e de H obtemos dois componentes; como G é conexo, ele tem uma aresta f conectando esses dois componentes. A aresta f não pode ser mais cara que e, do contrário o governo pessimista teria escolhido f para eliminar ao invés de e. Mas então podemos substituir e por f em H sem aumentar seu custo. Donde concluimos como na prova dada acima.

9.2. [Muito semelhante.]

9.3. [Muito semelhante.]

9.4. Tome nós $1, 2, 3, 4$ e custos $c(12) = c(23) = c(34) = c(41) = 3$, $c(13) = 4$, $c(24) = 1$. O governo pessimista constrói (12341), enquanto que a melhor solução é 12431.

9.2 Caixeiro Viajante

9.5. Não, porque ele intersecta a si próprio (veja o próximo exercício).

9.6. Substituindo duas arestas que se intersectam por duas outras arestas ligando dois-a-dois os mesmos 4 nós, justamente de modo diferente, dá uma caminhada mais curta pela desigualdade triangular.

10 Casamentos em grafos

10.1 Um problema de dança

10.1. Se todo grau é d, então o número de arestas é $d \cdot |A|$, mas também $d \cdot |B|$.

10.2. (a) Um triângulo; (b) uma estrela.

10.3. Um grafo no qual todo nó tem grau 2 é a união de ciclos disjuntos. Se o grafo é bipartite, esses ciclos têm comprimento par.

10.3 O teorema principal

10.4. Suponha que $X \subseteq A$ e que Y denote o conjunto de vizinhos de X em B. Existem exatamente $d|X|$ arestas começando de X. Todo nó em Y acomoda não mais que d desses; donde $|Y| \geq |X|$.

10.5. A suposição para $X = A$ resulta que $|B| \geq |A|$. Se $|B| = |A|$ então já sabemos a asserção (Teorema 10.3.1), portanto suponha que $|B| > |A|$. Adicione $|B| - |A|$ novos nós a A, para obter um conjunto A' com $|A'| = |B|$. Conecte todo novo nó a todo nó em B. O grafo que obtemos satisfaz as condições no Teorema do Casamento 10.3.1: temos $|A'| = |B|$, e se $X \subseteq A'$ então ou $X \subseteq A$ (caso em que ele tem pelo menos $|X|$ vizinhos em B pela suposição do exercício), ou X contém um novo nó, caso em que todo nó em B é um vizinho de X. Portanto o novo grafo tem um casamento perfeito. Removendo os nós recentemente adicionados, as arestas do casamento perfeito que permanece casa todos os nós de A com diferentes nós de B.

10.4 Como encontrar um casamento perfeito?

10.6. Sobre um caminho com 4 nós, podemos selecionar a aresta do meio.

10.7. As arestas no casamento guloso M têm que tocar toda aresta em G (caso contrário, poderíamos estender ainda mais M), em particular toda aresta no casamento perfeito. Portanto toda aresta no casamento perfeito tem no máximo uma extremidade não-casada por M.

10.8. O maior casamento tem 5 arestas.

10.9. Se o algoritmo termina sem um casamento perfeito, então o conjunto S mostra que o grafo não é "bom".

11 Combinatória em Geometria

11.1 Interseções de diagonais

11.1. $\frac{n(n-3)}{2}$.

11.2 Contando regiões

11.2. Verdadeiro para $n = 1$. Seja $n > 1$. Remova qualquer reta. As retas remanescentes dividem o plano em $(n-1)n/2 + 1$ regiões pela hipótese da indução. A última reta corta n dessas em duas. Portanto obtemos

$$\frac{(n-1)n}{2} + 1 + n = \frac{n(n+1)}{2} + 1.$$

11.3 Polígonos convexos

11.3. Veja a Figura 16.1.

12 Fórmula de Euler

12.1 Um planeta sob ataque

12.1. Existem n nós de grau $n-1$ e $\binom{n}{4}$ nós de grau 4 (ver seção 11.1). Portanto o número de arestas é $\frac{1}{2}\left(n \cdot (n-1) + \binom{n}{4} \cdot 4\right)$. Da Fórmula de Euler, o número de países é

$$\left(2\binom{n}{4} + \binom{n}{2}\right) - \left(n + \binom{n}{4}\right) + 2 = \binom{n}{4} + \binom{n}{2} - n + 2;$$

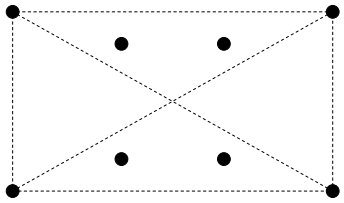

Figura 16.1:

você tem que subtrair 1 para o país do lado de fora.

12.2. Seja f o número de regiões da ilha. Considere o grafo formado pelas barragens e também a fronteira da ilha. Existem $2n$ nós de grau 3 (ao longo da praia), e $\binom{n}{2}$ nós de grau 4 (os pontos de interseção de barragens retas). Portanto o número de arestas é

$$\frac{1}{2}\left((2n)\cdot 3 + \binom{n}{2}\cdot 4\right) = 2\binom{n}{2} + 3n.$$

O número de países é $f+1$ (temos que contar o oceano também), portanto a fórmula de Euler dá $f + 1 + 2n + \binom{n}{2} = 2\binom{n}{2} + 3n + 2$, donde $f = \binom{n}{2} + n + 1$.

12.2 Grafos planares

12.3. Sim,

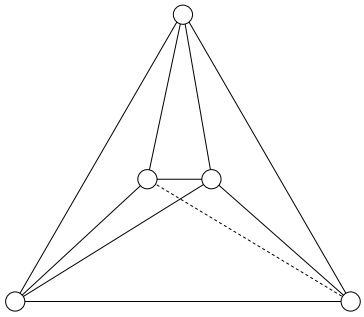

Figura 16.2:

12.4. Não; o argumento é similar ao que mostra que K_5 não é planar. As casas, cacimbas e caminhos formam um grafo bipartite com 6 nós e 9 arestas. Suponha que isso pode ser desenhado no plano sem interseções. Então temos $9+2-6 = 5$ regiões. Cada região tem pelo menos 4 arestas (pois não existem triângulos), e portanto o número de arestas é pelo menos $\frac{1}{2}\cdot 5\cdot 4 = 10$, o que é uma contradição.

13 Colorindo mapas e grafos

13.1 Colorindo regiões: um caso simples

13.1. Por indução. Verdadeiro se $n = 1$. Seja $n > 1$. Assuma que a descrição da coloração seja válida para os primeiros $n - 1$ círculos. Se adicionarmos o n-ésimo, a cor e a paridade não mudam fora desse círculo; ambas mudam dentro do círculo. Portanto a descrição permanece válida.

13.2. (a) Por indução. Verdadeiro para 1 reta. Adicionando um reta, re-colorimos todas as regiões em um lado.
(b) Uma possível descrição: designe uma direção como "para cima". Seja p um ponto qualquer que não está sobre qualquer das retas. Comece uma semi-reta "para cima" a partir de p. Conte quantas das retas dadas a intersectam. Pinte de acordo com a paridade desse número de interseção.

13.1 Colorindo grafos com duas cores

13.3. Esse grafo não pode conter qualquer ciclo ímpar. De fato, se considerarmos qualquer ciclo C, então cada aresta dele contém exatamente um ponto de interseção com a união de círculos. A contribuição de todo círculo é par, pois caminhando em torno de C, cruzamos o o círculo alternando dentro e fora.

13.3 Colorindo grafos com muitas cores

13.4. Suponha que tenhamos um boa 3-coloração do primeiro grafo. Começando de cima, o primeiro vértice recebe (digamos) a cor 1, os vértices no segundo nível têm que receber cores 2 e 3, e então ambos os vértices mais inferiores têm que receber a cor 1. Mas isso é impossível, pois eles estão conectados.
Suponha que tenhamos uma boa 3-coloração do segundo grafo. Começando do centro, podemos assumir que ele tem a cor 1, portanto seus vizinhos recebem as cores 2 ou 3. Agora repinte cada vértice externo com a cor 1 dando-lhe a cor de seu "gêmeo" interno. Essa coloração daria uma boa de um 5-cicle por meio de 2 cores, pois "gêmeos" têm os mesmos vizinhos (exceto que o gêmeo interno está também conectado ao centro). Isso é uma contradição.

13.5. Rotacionando o plano um pouco, podemos assumir que todos os pontos de interseção têm diferentes coordenadas y (as quais chamamos simplesmente "alturas"). Começando com o ponto de interseção mais alto, e movendo para baixo, podemos colorir os pontos de interseção um por um. Cada vez existem no máximo dois pontos de interseção que são adjacentes ao ponto corrente ao longo das duas retas que foram coloridos previamente, e portanto podemos encontrar uma cor para o ponto corrente diferente dessas.

13.6. Podemos assumir que existem pelo menos 2 nós, e portanto existe um nó de grau no máximo d. Removemo-lo, recursivamente colorirmos o grafo remanescente com $d + 1$ cores, e então podemos estender essa coloração para o último ponto, pois seus d vizinhos excluem apenas d cores.

13.7. Removemos um ponto de grau d, e recursivamente colorimos o grafo remanescente com $d + 1$ cores. Podemos estender este como na solução anterior.

13.4 Coloração de Mapas e o Teorema das Quatro Cores

14 Geometrias finitas, códigos, quadrados latinos, e outras belas criaturas

14.1 Pequenos mundos exóticos

14.1. O próprio plano de Fano.

14.2. Seja abc um círculo. Então duas retas por a contêm b e c, respectivamente, portanto elas não são tangentes. A terceira reta por a é a tangente.

14.3. Se H é um hipercírculo, então seus 4 pontos determinam 6 retas, e 3 dessas 6 linhas passam por cada um dos seus pontos. Portanto a sétima reta não passa por qualquer dos 4 pontos do hipercírculo. Reciprocamente, se L é uma reta, então os 4 pontos que não estão sobre L não podem conter uma outra reta (do contrário, essas duas retas não intersectariam), e portanto essse 4 pontos formam um hipercírculo.

14.4. (a) Se todo mundo sobre a reta L vota SIM, então (como toda reta intersecta L) toda reta tem pelo menos um ponto votando SIM, e portanto nenhuma reta votará tudo-NÃO. (b) Podemos assumir que pelo menos 4 pontos votam SIM; sejam a, b, c e d 4 deles. Suponha que não exista reta votando tudo-SIM. Então cada uma das 3 retas por a contém no no máximo um voto SIM a mais, portanto cada uma delas tem que conter exatamente um dos pontos b, c e d. Portanto os 3 pontos remanescentes votam NÃO. Os votos SIM formam um hipercírculo (exercício 14.3), portanto os votos NÃO formam uma reta.

14.5. (a) Através de dois pontos originais, existe a reta original; através de um ponto original a e um novo ponto b, existe uma única reta por a entre todas as retas paralelas para as quais b foi adicionado; e para dois novos pontos, existe a nova reta. (b) é semelhante. (c) é obvio. (d) segue de (a)-(b)-(c), como vimos acima.

14.6. Sim: para toda reta (2 pontos) existe exatamente uma reta que é disjunta dela (os outros 2 pontos).

14.7. Veja a Figura 16.3 (existem muitas outras maneiras de mapear os pontos)

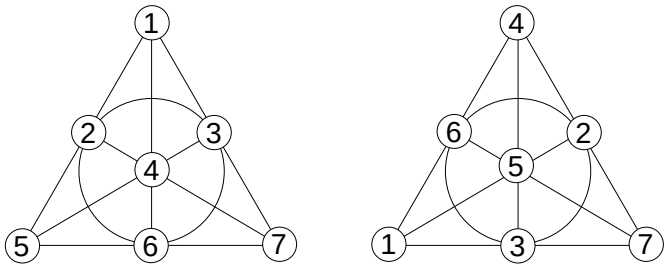

Figura 16.3:

14.8. Isso não é uma coincidência. Fixe qualquer ponto A do espaço Cubo. Todo plano por A contém 3 retas por A. Se chamarmos as retas por um dado ponto "PONTOS", e aquelas triplas dessas retas que pertencem a um plano "RETAS", então aqueles PONTOS e RETAS formam um plano de Fano.

14.2 Planos finitos afins e projetivos

14.9. Fixe qualquer ponto a. Existem $n + 1$ retas por a, que não têm outros pontos em comum e cubra o plano inteiro por (a). Cada uma dessas retas tem n pontos além de a,

portanto existem $(n+1)n$ pontos além de a, e $n(n+1)+1 = n^2+n+1$ pontos no total.

14.10. Podemos atribuir coordinadas aos vértices do cubo como se fosse no espaço euclideano, mas pense nas coordenadas como elementos do corpo de 2-elementos (Figura 16.4). Então é fácil (embora demorado) verificar que os planos do espaço Cubo são precisamente os conjuntos de pontos dados pelas equações lineares. Por examplo, a equação linear $x+y+z=1$ dá os pontos $001,\ 010,\ 011,\ 111$ (não esquecer, estamos trabalhando no corpo de 2-elementos), que é exatamente o plano consistindo dos pontos claros.

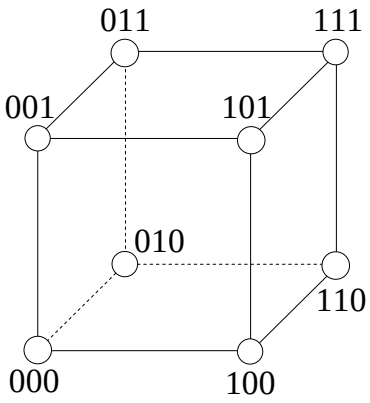

Figura 16.4:

14.11. Um plano projetivo de ordem 10 deve ter $10^2+10+1 = 111$ pontos, 111 retas, com 11 pontos sobre cada reta. O número de maneiras de selecionar uma reta candidata é $\binom{111}{11}$; o número de maneiras de selecionar 111 retas candidatas é

$$\binom{\binom{111}{11}}{111} = \binom{473239787751081}{11} > 10^{1448}.$$

Poder-se-ia não verificar tantas possibilidades mesmo com o computador mais rápido no tempo de vida do universo! Lam, Thiel e Swiercz tiveram que trabalhar de uma maneira muito mais sofisticada.

14.3 Desenhos em bloco

14.12. 441, 44.

14.13. Para quaisquer dois cidadãos C e D, existem λ clubes contendo ambos. Se totalizarmos isso para todo D, contamos $(v-1)\lambda$ clubes contendo C. Cada clube desses é contado $k-1$ times (uma vez para cada membro diferente de C, portanto o número de clubes contendo C é $(v-1)\lambda/k$. Isso é o mesmo para todo cidadão C.

14.14. (a) $v=6$, $r=3$, $k=3$ dá $b=6$ por (14.1), mas $\lambda = 6/5$ por (14.2). (b) $b=8$, $v=16$, $r=3$, $k=6$, $\lambda=1$ (existem muitos outros exemplos em ambos os casos).

14.15. Tome $b = v$ clubes, e construa para todo cidadão C um clube no qual todo mundo é um membro exceto C. Então $b = v$, $k = v - 1$, $r = v - 1$, $\lambda = v - 2$.

14.4 Sistemas de Steiner

14.16. Sejam A, B, C 3 elementos que não formam um clube. Existe um único clube contendo A e B, que tem um único terceiro elemento; chame esse de D. Igualmente, existe um único elemento E tal que ACE é um clube, e um único elemento F tal que BCF é um clube. Os elementos D, E, F têm que ser distintos, pois se (digamos) $D = E$, então A e D estão contidos nos dois clubes (um com B e um com C). Suponha que o sétimo elemento seja G. Existe um único clube contendo C e D, e o terceiro membro desse clube tem que ser G (podemos verificar que qualquer das outras 4 escolhas resultaria em dois clubes com dois membros em comum). Igualmente, AFG e BEG são clubes. Igualmente, existe um único clube contendo D e E, cujo terceiro membro tem que ser F. Portanto, exceto pelos nomes dos cidadãos, a estrutura de clube é univocamente determinada.

14.17. Temos $r = (v - 1)/2$ por (14.2), e daí $b = v(v - 1)/6$ por (14.1). Como $v - 1 \geq 6$, temos que $b \geq v$.

14.18. Chame uma tripla contida em S de S-tripla. O número total de triplas é $b = v(v - 1)/6$, o número de S-triplas é

$$b' = \frac{\frac{v-1}{2}\left(\frac{v-1}{2} - 1\right)}{6} = \frac{(v-1)(v-3)}{24},$$

e portanto o número de não-S-triplas é $b - b' = \frac{(v+1)(v-1)}{8}$. Toda não-$S$-tripla tem no máximo um ponto em S e por conseguinte no mínimo dois pontos que não estão em S. Mas o número de pares que não estão em S é $\binom{(v+1)/2}{2} = \frac{(v+1)(v-1)}{8}$, e como esses pares podem pertencer a somente uma das não-S-triplas, segue que cada uma das não-S-triplas tem que conter exatamente um par de elementos fora de S. Isso prova que cada não-S-tripla tem que conter um elemento de S.

14.19. Veja a Figura 16.5.

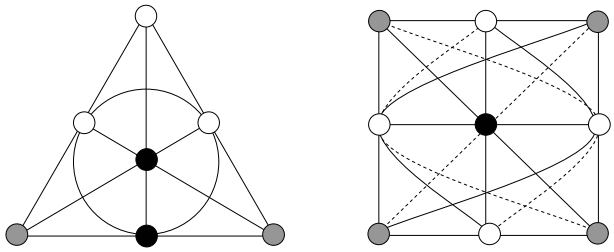

Figura 16.5:

14.20. Toda garota tem outras 8 garotas com quem caminhar, todo dia ela pode caminhar com 2 numa linha. Portanto 4 dias são necessários para ela caminhar com todo mundo exatamente uma vez.

14.5 Quadrados latinos

14.21. Existem 576 quadrados latinos 4×4 diferentes. Existem muitas maneiras de se chegar a esse número; esboçamos uma. A primeira linha pode ser preenchida de $4!$ maneiras. Essas são todas equivalentes no sentido de que o número de maneiras pelas quais elas podem ser completadas é o mesmo para cada uma delas, portanto podemos fixar a primeira linha em 0 1 2 3 e simplesmente contar o número de maneiras para completar esta. A primeira coluna agora pode ser preenchida de $3!$ maneiras, e novamente todas essas são equivalentes, portanto vamos fixá-la em 0 1 2 3.
Se o 0 na segunda linha está na segunda posição, então o restante da segunda linha e da segunda coluna é forçado, mas obtemos duas maneiras de preencher os 4 campos no canto inferior direito. Se o 0 na segunda linha está na terceira ou quarta posição, então a maneira de preencher o restante é forçado. Portanto obtemos os 4 quadrados latinos abaixo:

0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
1	0	3	2	1	0	3	2	1	2	3	0	1	3	0	2
2	3	0	1	2	3	1	0	2	3	0	1	2	0	3	1
3	2	1	0	3	2	0	1	3	0	1	2	3	2	1	0

Por conseguinte o número de maneiras de preencher os 9 corpos remanescentes é 4, portanto o número total é $4! \cdot 3! \cdot 4 = 576$.
Essas quatro podem parecer diferentes, mas se trocarmos 1 e 2 na terceira, intercambiarmos linhas 2 e 3, e intercambiarmos columas 2 e 3, obtemos a segunda. Igualmente, se intercambiarmos 1 e 3 na quarta, intercambiarmos linhas 2 e 4, e intercambiarmos columas 2 e 4, obtemos a segunda. Portanto as últimas 3 dessas não são essencialmente diferentes.
Não há maneira de obter o segundo quadrado a partir do primeiro por meio de tais operações (isso segue e.g. pelo exercício 14.27). Portanto esses são dois quadrados latinos 4×4 essencialmente diferentes.

14.22. Isso é bem simples. Por exemplo, a tabela abaixo é boa (existem muitas outras possibilidades):

$$\begin{array}{cccccc} 0 & 1 & 2 & \dots & n-2. & n-1 \\ 1 & 2 & 3 & \dots & n-1 & 0 \\ 2 & 3 & 4 & \dots & 0 & 1 \\ \vdots & & & & & \vdots \\ n-1 & 0 & 1 & \dots & n-3 & n-2 \end{array}$$

14.23.

1	2	3	1	2	3
2	3	1	3	1	2
3	1	2	2	3	1

14.24. Adicionamos 1 a todo número, dessa maneira o total de toda linha e coluna aumenta de 4.

14.25. Precisamos de dois quadrados latinos onde não apenas nas linhas e colunas, mas também nas diagonais todo número ocorre uma vez. Esses dois servirão:

0	1	2	3		0	1	2	3
2	3	0	1		3	2	1	0
3	2	1	0		1	0	3	2
1	0	3	2		2	3	0	1

Desses dois obtemos o seguinte quadrado mágico perfeito:

0	5	10	15
11	14	1	4
13	8	7	2
6	3	12	9

c

14.26. Se existe tal quadrado latino, então arbitrariamente permutando os números 0,1,2,3 nele daria um outro quadrado ortogonal aos três quadrados em (14.9) e (14.12). (Prove!) Portanto podemos começar com um quadrado tendo sua primeira linha 0 1 2 3. Mas então o que pode ser sua primeira entrada na segunda linha? 0 é impossível (porque a entrada acima dela também é 0), mas 1, 2 ou 3 estão também descartados: por exemplo se tivéssemos 2, então não seria ortogonal ao quadrado (14.12), porque o par (2,2) ocorreria duas vezes. Portanto não existe tal quadrado latino. (Tente generalizar esse resultado: dos $n \times n$ quadrados latinos, podemos escolher no máximo $n - 1$ quadrados ortogonais dois-a-dois um ao outro.)

14.27. Se tivéssemos um quadrado ortogonal a (14.13), então usando o mesmo argumento que na solução do exercício 14.26, podemos supor que a primeira linha é 0 1 2 3. Então os pares (0,0), (1,1), (2,2) e (3,3) ocorrem na primeira linha, o que implica que nas outras linhas, os dois quadrados não podem ter o mesmo número na mesma posição.
Em particular, a primeira entrada na segunda linha não pode ser 1, e ela não pode ser 0 (porque a entrada acima dela é 0). Então ela é 2 ou 3.
Suponha que ela seja 2. Então a segunda entrada nessa linha não pode ser 1 ou 2 (existe um 1 acima dela e um 2 antes dela), e não pode ser 3, portanto ela é 0. A quarta entrada não pode ser 2,0 ou 3, portanto ela tem que ser 1; segue que a segunda linha é 2 0 3 1 (o mesmo que a terceira linha em (14.13)). A seguir podemos adivinhar a última linha: cada entrada é diferente das duas acima dela na primeira e segunda linha, e também da última linha de (14.13), o que implica que essa linha tem que ser o mesmo que a segunda linha de (14.13): 1 3 0 2. Daí a terceira linha tem que ser 3 2 1 0; mas agora o par (3,1) ocorre duas vezes quando as duas últimas linhas são superpostas.
O caso em que a segunda linha começa com um 3 pode ser argumentado da mesma maneira.

14.6 Códigos

14.28. Suponha que um código é d-error-corretor. Afirmamos que para quaisquer duas palavras-código, temos que inverter no mínimo least $2d + 1$ bits para chegar de uma para outra. De fato, se pudéssemos chegar de uma palavra-código u à palavra-código v invertendo apenas $2d$ bits, então considere a palavra-código w obtida de u invertendo-se d desses bits. Poderíamos receber w ao invés de u, mas também ao invés de v, de modo que o código não é d-error-corretor.
Agora se recebemos qualquer mensagem que tem no máximo $2d$ erros, então essa mesnagem não é uma outra palavra-código, portanto podemos detectar até $2d$ erros.

A recíproca é provada de modo similar.

14.29. Se a cadeia não tem 1's, então ela é uma palavra-código. Se ela contém um 1, esse pode ser invertido para se obter uma palavra-código. Se ela tem dois 1's, então existe uma linha através dos dois pontos correspondentes do plano de Fano, e invertendo-se o 0 na posição correspondente ao terceiro ponto dá uma palavra-código. Se ela tem três 1's, e esses são colineares, então ela é uma palavra-código. Se ela tem três 1's, e esses não são colineares, então existe um único ponto que não está sobre qualquer das três linhas determinadas por eles, e invertendo-se esse obtemos uma palavra-código. Se ele contém pelo menos quatro 1's, então podemo argumentar de modo similar, intercambiando o papel de 1's e 0's.

15 Uma olhadela em complexidade e criptografia

15.2 Criptografia clássica

15.1. I THINK WE SHOULD NOT ATTACK FOR ANOTHER WEEK, BUT THEN WITH FULL FORCE. BELA

15.2. Seja $a_1a_2\ldots a_n$ a chave e $b_1b_2\ldots b_n$, o texto-pleno. Caligula intercepta uma mensagem cujos bits são $a_2 \oplus b_1, a_3 \oplus b_2, \ldots a_n \oplus b_{n-1}$, e uma outra mensagem cujos bits são $a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n$. (A segunda mensagem é um bit mais longa, o que pode lhe dar uma dica do que aconteceu.) Ele pode computar a soma binária dos primeiros bits, segundos bits, etc. Portanto ele obtém $(a_2 \oplus b_1) \oplus (a_1 \oplus b_1) = a_1 \oplus a_2$, $(a_3 \oplus b_2) \oplus (a_2 \oplus b_2) = a_2 \oplus a_3$, etc.
Agora ele adivinha que $a_1 = 0$; como ele conhece $a_1 \oplus a_2$, ele pode computar a_2, então igualmente a_3, e assim por diante, ele obtém a chave inteira. Pode ser que seu palpite inicial estava errado, o que ele nota pois tentando decodificar a mensagem ele obtém lixo; mas então ele pode tentar $a_1 = 1$, e recuperar a chave. Um dos dois palpites funcionará.

15.3. Seja $a_1a_2\ldots a_n$ a chave e suponha que $b_1b_2\ldots b_n$ e $c_1c_2\ldots c_n$ sejam os dois textos-plenos. Caligula intercepta uma mensagem cujos bits são $a_1 \oplus b_1, a_2 \oplus b_2, \ldots a_n \oplus b_n$, e uma outra mensage cujos bits são $a_1 \oplus c_1, a_2 \oplus c_2, \ldots, a_n \oplus c_n$. Como antes, ele computa a soma binária dos primeiros bits, segundos bits, etc., para obter $(a_1 \oplus b_1) \oplus (a_1 \oplus c_1) = b_1 \oplus c_1$, $(a_2 \oplus b_2) \oplus (a_2 \oplus c_2) = b_2 \oplus c_2$, etc.
O resto não é tão imediato como no exercício anterior, mas suponha que Caligula pode adivinhar parte da (digamos) mensagem de Arthur (assinatura, ou endereço, ou algo semelhante). Então, como ele conhece a soma binária bit-a-bit das duas mensagens, ele pode recuperar a parte correspondente da mensagem de Bela. Com alguma sorte, essa não é uma frase inteira, e contém parte de uma palavra. Então ele pode adivinhar o resto da palavra, e isso lhe dá algumas poucas letras a mais da mensagem de Arthur. Com alguma sorte, isso sugere algumas letras a mais da mensagem de Bela, etc.
Isso não é completamente imediato, mas tipicamente dá informação suficiente para decodificar as mensagens (como os quebradores de código da Segunda Grande Guerra aprenderam). Um ponto importante: Caligula pode *verificar* que essa reconstrução está correta, pois nesse caso ambas as mensagens têm que acabar significando algo.

15.3 Como salvar o último movimento em xadrez?

15.4. Alice pode facilmente tapear: ela pode enviar simplesmente uma cadeia aleatória x à noite, pensar no seu movimento durante a noite, juntamente com a cadeia y que o codifica, e enviar a soma binária de x e y como a suposta chave.

15.5. Isso certamente elimina a tapeação no exercício anterior, pois se ela muda de opinião, a "chave" que ela calcula de volta da mensagem na manhã seguinte não terá significado. Mas agora Bob tem a vantatem: ele pode tentar can todos as chaves "aleatórias mas com significado", pois não há muitas delas.

15.6 Criptografia de chave pública

15.6. (a) Escolha aleatoriamente números (chaves públicas) $e_1, e_2, \ldots e_M$ e aplique o algoritmo hipotetizado para computar as chaves secretas correspondentes $d_1, d_2, \ldots, d_M$. O número $k = (p-1)(q-1)$ é um divisor comum de $e_1d_1 - 1, e_2d_2 - 1, \ldots, e_Md_M - 1$, portanto ele é um divisor de $K = \mathrm{mdc}(e_1d_1 - 1, e_2d_2 - 1, \ldots, e_Md_M - 1)$, o qual podemos computar. Se $K < m$, então sabemos que na verdade $k = K$, pois $k = (p-1)(q-1) > pq/2 = m/2$. Caso contrário escolhemos uma outra chave pública e_{M+1} e repetimos. Pode-se mostrar que após não mais do que cerca de $\log m$ iterações, encontramos k com alta probabilidade.
(b) Se conhecemos $m = pq$ e $k = (p-1)(q-1)$, então conhecemos $p+q = m-k+1$, e portanto p e q podem ser determinados como as soluções da equação quadrática $x^2 - (m-k+1)x + m = 0$.

Índice Remissivo