Capítulo 16

Repostas 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) Powers of 2. (b) $2^n - 1$. (c) sets not containing the last element.

1.23. 2^{n-1}.

1.24. Divide all subsets into pairs, so that each pair differs only in their first element. Each pair contains an even and an odd subset, so their numbers are the same.

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 Sequences

1.28. The trees have 9 and 12 leaves, respectively.

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 Permutations

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 The number of ordered subsets

1.36. (We don't think you could really draw the whole tree; it has almost 10^{20} leaves. It has 11 levels of nodes.)

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. In one case, repetition is not allowed, while in the other case, it is allowed.

1.8 The number of subsets of a given size

1.40. Handshakes; lottery; hands in bridge.

1.41. See Pascal's Triangle in Chapter 3.

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

1.43. An algebraic proof of (1.7) is straightforward. In (1.8), the right hand side counts k-subsets of an n-element set by separately counting those that contain a given element and those that do not.

1.44. An algebraic proof is easy. A combinatorial interpretation: n^2 is the number of all ordered pairs (a, b) with $a, b \in \{1, 2, \ldots, n\}$. $\binom{n}{2}$ is the number of ordered pairs (a, b) among these with $a < b$ (why?). To count the remaining ordered pairs (a, b) (those with $a \geq b$), add 1 to their first entry. Then we get a pair (a', b) with $1 \leq a', b \leq n + 1$, $a' > b$, and vice versa, every such pair is obtained this way. Hence the number of these pairs is $\binom{n+1}{2}$.

1.45. Again, an algebraic proof is easy. A combinatorial interpretation: We can choose a k-element set by first choosing one element (n possibilities) and then choosing a $(k-1)$-element subset of the remaining $n-1$ elements ($\binom{n-1}{k-1}$ possibilities). But we get every k-element subset exactly k times (depending on which of its elements was chosen first), so we have to divide the result by k.

1.46. Both sides count the number of ways to divide an a-element set into three sets with $a - b$, $b - c$, and c elements.

2 Combinatorial tools

2.1 Induction

2.1. One of n and $n + 1$ is even, so the product $n(n + 1)$ is even. By induction: true for $n = 1$; if $n > 1$ then $n(n + 1) = (n - 1)n + 2n$, and $n(n - 1)$ is even by the induction hypothesis, $2n$ is even, and the sum of two even numbers is even.

2.1. True for $n = 1$. If $n > 1$ then

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

2.2. The youngest person will count n handshakes. The 7-th oldest will count 6 handshakes. So they count $1 + 2 + \ldots + n$ handshakes. We already know that there are $n(n + 1)/2$ handshakes.

2.3. Compute the area of the rectangle in two different ways.

2.4. By induction on n. True for $n = 2$. For $n > 2$, we have

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

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

2.5. If n is even, then $1 + n = 2 + (n - 1) = \ldots = \left(\frac{n}{2} - 1\right) + \frac{n}{2} = n + 1$, so the sum is $\frac{\frac{n}{2}(n+1) = n(n+1)}{2}$. If n is odd then we have to add the middle term separately.

2.6. If n is even, then $1 + (2n-1) = 3 + (2n-3) = \ldots = (n-1) + (n+1) = 2n$, so the sum is $\frac{n}{2}(2n) = n^2$. Again, is n is odd the solution is similar, but we have to add the middle term separately.

2.7. By induction. True for $n = 1$. If $n > 1$ then

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

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

2.8. By induction. True for $n = 1$. If $n > 1$ then

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

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

2.9. (Strings) True for $n = 1$. If $n > 1$ then to get a string of length n we can start with a string of length $n-1$ (this can be chosen in k^{n-1} ways by the induction hypothesis) and append an element (this can be chosen in k ways). So we get $k^{n-1} \cdot k = k^n$.
(Permutations) True for $n = 1$. To seat n people, we can start with seating the oldest (this can be done in n ways) and then seating the rest (this can be done in $(n-1)!$ ways be the induction hypothesis). We get $n \cdot (n-1)! = n!$.

2.10. True if $n = 1$. Let $n > 1$. The number of handshakes between n people is the number of handshakes by the oldest person (this is $n-1$) plus the number of handshakes between the remaining $n-1$ persons (which is $(n-1)(n-2)/2$ by the induction hypothesis). We get $(n-1) + (n-1)(n-2)/2 = n(n-1)/2$ handshakes.

2.11. We did not check the base case $n = 1$.

2.12. The proof uses that there are at least four lines. But we only checked $n = 1, 2$ as base cases. The assertion is false for $n = 3$ and for every value of n after that.

2.2 Comparing and estimating numbers

2.13. (a) the left hand side counts all subsets of an n-set, the right hand side counts only the 3-element subsets. (b) $2^n/n^2 > \binom{n}{3}/n^2 = (n-1)(n-2)/(6n)$, which becomes arbitrarily large.

2.14. Start the induction with $n = 4$: $4! = 24 > 16 = 2^4$. If the inequality holds for n, then $(n+1)! = (n+1)n! > (n+1)2^n > 2 \cdot 2^n = 2^{n+1}$.

2.3 Inclusion-exclusion

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

2.4 Pigeon holes

2.16. If each of the giant boxes contains at most 20 New Yorkers, then 500,000 boxes contain at most $20 \cdot 500,000 = 10,000,000$ New Yorkers, which is a contradiction.

3 Binomial coefficients and Pascal's Triangle

3.1 The Binomial Theorem

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) By $\binom{n}{k} = \binom{n}{n-k}$.

3.3. The identity says that *the number of subsets of an n-element set with an even number of elements is the same as the number of subsets with an odd number of elements.* We can establish a bijection between even and odd subsets as follows: if a subset contains 1, delete it from the subset; else, add it to the subset.

3.2 Distributing presents

3.4.

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

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

3.5. (a) $n!$ (distribute positions instead of presents). (b) $n(n-1)\ldots(n-k+1)$ (distribute as "presents" the first k positions at the competition and $n-k$ certificates of participation). (c) $\binom{n}{n_1}$. (d) Chess seating in Diane's sense (distribute players to boards).

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

3.3 Anagrams

3.7. $13!/2^3$.

3.8. COMBINATORICS.

3.9. Most: any word with 13 different letters; least: any word with 13 identical letters.

3.10. (a) 26^6.
(b) $\binom{26}{4}$ ways to select the four letters that occur; for each selection, $\binom{4}{2}$ ways to select the two letters that occur twice; for each selection, we distribute 6 positions to these letters (2 of them get 2 positions), this gives $\frac{6!}{2!2!}$ ways. Thus we get $\binom{26}{4}\binom{4}{2}\frac{6!}{2!2!}$. (There are many other ways to arrive at the same number!)
(c) Number of ways to partition 6 into the sum of positive integers:

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

which makes 11 possibilities.
(d) This is too difficult in this form. What we meant is the following: how many words of length n are there such that none is an anagram of another? This means distributing n pennies to 26 children, and so the answer is $\binom{n+25}{25}$.

3.4 Distributing money

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 Pascal's Triangle

3.14. This is the same as $\binom{n}{k} = \binom{n}{n-k}$.

3.15. $\binom{n}{0} = \binom{n}{n} = 1$ (e.g. by the general formula for the binomial coefficients).

3.6 Identities in the Pascal Triangle

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. The coefficient of $x^n y^n$ in

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

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. The left hand side counts all k-element subsets of an $(n+m)$-element set by distinguishing them according to how many elements they pick up from the first n.

3.19. If the largest element is j (which is at least $n+1$), then the rest can be chosen $\binom{j-1}{n}$ ways. If we sum for all $j \geq n+1$, we get the identity

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

Using that $\binom{n+i}{n} = \binom{n+i}{i}$, we get (3.5).

3.7 A bird's eye view at the Pascal Triangle

3.20. $n = 3k+2$.

3.21. This is not easy. Look at the difference of differences:

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

We want to determine the first value of k where it turns negative. we can divide the expression by $\binom{n}{k-1}$ and multiply by $k(k+1)$ to get

$$(n-k+1)(n-k) - 2(n-k+1)(k+1) + k(k+1) \;\stackrel{?}{\;}\; 0.$$

Simplifying,

$$4k^2 - 4nk + n^2 - n - 2 \;\stackrel{?}{\;}\; 0.$$

Solving for k, we get that the left hand side is nonpositive between the two roots:

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

So the first integer k for which this is nonpositive is

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

3.22. (a) We have to show that $e^{-t^2/(m-t+1)} \leq e^{-t^2/m} \leq e^{-t^2/(m+t)}$. This is straightforward using that e^x is a monotone increasing function.
(b) Take the ratio of the upper and lower bounds:

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

Here the exponent is

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

In our case, this is $1900/(41*60) \approx .772$, and so the ratio is $e^0.772 \approx 2.1468$.

3.23. By (3.9), we have

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

Here the exponent is a monotone increasing function of t for $t \geq 0$ (to see this, write it as $t(1-\frac{m}{m+t})$, or take its derivative), and so from our assumption that $t \geq \sqrt{m \ln C} + \ln C$ it follows that

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

which implies that

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

The proof of the other half is similar.

4 Fibonacci numbers

4.1 Fibonacci's exercise

4.1. Because we use the two previous elements to compute the next.

4.2. F_{n+1}.

4.3. Let us denote by S_n the number of good subsets. If n=1, then $S_1 = 2$ (the empty set and the set $\{1\}$. If $n = 2$, then $\emptyset$, $\{1\}$, $\{2\}$, so S_2=3. For any n if the subset contains n, then it can not contain $n-1$, so there are S_{n-2} subsets of this type, if it does not contain n, then there are S_{n-1} subsets. So we have the same recursive formula, so $S_n = F_{n+2}$.

4.2 Lots of identities

4.4. It is clear from the recurrence that two odd members are followed by an even, then by two odd numbers again.

4.5. We formulate the following nasty looking statement: *if n is divisible by 5, then so is F_n; if n has remainder 1 when divided by 5, then F_n has remainder 1; if n has remainder 2 when divided by 5, then F_n has remainder 1; if n has remainder 3 when divided by 5, then F_n has remainder 2; if n has remainder 4 when divided by 5, then F_n has remainder 3.* This is then easily proved by induction on n.

4.6. By induction. All of them are true for $n = 1$ and $n = 2$. Assume that $n \geq 3$.

(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. We can write (4.1) as $F_{n-1} = F_{n+1} - F_n$, and use this to compute F_n for negative n recursively (going backwards):

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

It is easy to recognize that these are the same as the ordinary Fibonacci numbers, except that every second has a negative sign. In formula,

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

This is now easily proved by induction on n. It is true for $n = 0, 1$, and assuming that it is true for n and $n-1$, we get for $n+1$:

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

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

which completes the induction.

4.8.

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

Replacing n by $2n-1$, we get the recurrence for odd-index Fibonacci numbers. Using this to prove (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. The identity is

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

where $k = \lfloor n/2 \rfloor$. Proof by induction. True for $n = 0$ and $n = 1$. Let $n \geq 2$. Assume that n is odd; the even case is similar, just the last term below needs a little different treatment.

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

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

4.10. (4.2) follows by taking $a = b = n-1$. (4.3), follows by taking $a = n$, $b = n-1$.

4.11. Let $n = km$. We use induction on m. For $m = 1$ the assertion is obvious. If $m > 1$, then we use (4.5) with $a = k(m-1)$, $b = k-1$:

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

By the induction hypothesis, both terms are divisible by F_a.

4.12. The "diagonal" is in fact a very long and narrow parallelogram with area 1. The trick depends on the fact $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ is very small compared to F_n^2.

4.3 A formula for the Fibonacci numbers

4.13. True for $n = 0, 1$. Let $n \geq 2$. Then by the induction hypothesis,

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

4.14. For $n = 1$ and $n = 2$, if we require that L_n is of the given form, then we get

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

Solving for a and b, we get

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

Then

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

which follows by induction on n just like in the previous problem.

4.15. (a) For example: every day Jack buys either an ice cream for \$1 or a giant sundae for \$2. There are 4 different favors of ice cream, but only one kind of sundae. If he has n dollars, in how many ways can he spend the money?

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

4.16. The formula works for $n = 1, 2 \ldots, 10$ but fails for $n = 11$, when it gives 91. In fact, it will be more and more off as we increase n. We have seen that

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

In the formula of Alice, the rounding plays less and less role, so

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

and so the ratio between Alice's numbers and the corresponding Fibonacci numbers is

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

Since the base of the exponential is larger than 1, this tends to infinity as n grows.

5 Combinatorial probability

5.1 Events and probabilities

5.1. The union of two events A and B corresponds to "A or B", i.e., at least one of A or B occurs.

5.2. It is the sum of some of the probabilities of outcomes, and even if add up all of the probabilities, we get just 1.

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

5.4. The same probabilities $\mathsf{P}(s)$ are added up on both sides.

5.5. Every probability $\mathsf{P}(s)$ with $s \in A \cap B$ is added twice to both sides; every probability $\mathsf{P}(s)$ with $s \in A \cup B$ but $s \notin A \cap B$ is added once to both sides.

5.2 Independent repetition of an experiment

5.6. The pairs $(E,T), (O,T), (L,T)$ are independent. The pair (E,O) is exclusive. Neither the pair (E,L) nor the pair (O,L) is independent.

5.7. $\mathsf{P}(\emptyset \cap A) = \mathsf{P}(\emptyset) = 0 = \mathsf{P}(\emptyset)\mathsf{P}(A)$. The set S also has this property: $\mathsf{P}(S \cap A) = \mathsf{P}(A) = \mathsf{P}(S)\mathsf{P}(A)$.

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. The probability that your mother has the same birthday as you is $1/365$ (here we assume that birthdays are distributed evenly among all numbers of the year, and we ignore leap years). These events are independent for your mother, father, and spouse, so the probability that for a given person, all three were born on his or her birthday is $1/365^3 = 1/48,627,125$. There are (roughly) 6 billion people in the word. Let's say 2 billion of them are married: we can expect $2,000,000,000/48,627,125 \approx 41$ of them have the same birthday as their mother, father, and spouse.

6 Integers, divisors, and primes

6.1 Divisibility of integers

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

6.2. (a) even; (b) odd; (c) $a = 0$.

6.3. (a) If $b = am$ and $c = bn$ then $c = amn$. (b) If $b = am$ and $c = an$ then $b + c = a(m + n)$ and $b - c = a(m - n)$. (c) If $b = am$ and $a, b > 0$ then $m > 0$, hence $m \geq 1$ and so $b \geq a$. (d) Trivial if $a = 0$. Assume $a \neq 0$. If $b = am$ and $a = bn$ then $a = amn$, so $mn = 1$. Hence either $m = n = 1$ or $m = n = -1$.

6.4. We have $a = cn$ and $b = cm$, hence $r = b - aq = c(m - nq)$.

6.5. We have $b = am$, $c = aq + r$ and $c = bt + s$. Hence $s = c - bt = (aq + r) - (am)t = (q - mt)a + r$. Since $0 \leq r < a$, the remainder of the division $s : a$ is 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 Factorization into primes

6.7. There is a smallest one among *positive* criminals (indeed, in every set of positive integers), but a set of negative integers need not have a smallest element (if it is infinite).

6.8. Yes, the number 2.

6.9. (a) p occurs in the prime factorization of ab, so it must occur in the prime factorization of a or in the prime factorization of b.
(b) $p|a(b/a)$, but $p \nmid a$, so by (a), we must have $p|(b/a)$.

6.10. Let $n = p_1 p_2 \ldots p_k$; each $p_i \geq 2$, hence $n \geq 2^k$.

6.11. If $r_i = r_j$ then $ia - ja$ is divisible by p. But $ia - ja = (i - j)a$ and neither a nor $i - j$ are divisible by p. Hence the r_i are all different. None of them is 0. Their number is $p - 1$, so every value $1, 2, \ldots, p - 1$ must occur among the r_i.

6.12. For a prime p, the proof is the same as for 2. If n is composite but not a square, then there is a prime p that occurs in the prime factorization of n an odd number of times. We can repeat the proof by looking at this p.

6.13. Fact: If $\sqrt[k]{n}$ is not an integer then it is irrational. Proof: there is a prime that occurs in the prime factorization of n, say t times, where $k \nmid t$. If (indirect assumption) $\sqrt[k]{n} = a/b$ then $nb^k = a^k$, and so the number of times p occurs in the prime factorization of the left hand side is not divisible by k, while the number of times it occurs in the prime factorization of the right hand side is divisible by k. A contradiction.

6.4 On the set of primes

6.14. Just as in the treatment of the case $k = 200$ above, we subtract the number of primes up to 10^{k-1} from the number of primes up to 10^k. By the Prime Number Theorem, this number is about

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

Since

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

is very close to 9 if k is large, we get that the number of primes with k digits is approximately

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

Comparing this with the total number of positive integers with k digits, which we know is $10^k - 10^{k-1} = 9 \cdot 10^{k-1}$, we get

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

6.5 Fermat's "Little" Theorem

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

6.16. (a) We need that each of the p rotated copies of a set are different. Suppose that there is a rotated copy which occurs a times. Then trivially every other rotated copy occurs a times. But then $a|p$, so we must have $a = 1$ or $a = p$. If all p rotated copies are the same, then trivially either $k = 0$ or $k = p$, which were excluded. So we have $a = 1$ as claimed. (b) Consider the set of two opposite vertices of a square. (c) If each box contains p subsets of size k, the total number of subsets must be divisible by p.

6.17. We consider each number to have p digits, by adding zeros at the front if necessary. We get p numbers from each number a by cyclic shift. These are all the same when all digits of a are the same, but all different otherwise (why? the assumption that p is a prime is needed here!). So we get $a^p - a$ numbers that are divided into classes of size p. Thus $p|a^p - a$.

6.18. Assume that $p \nmid a$. Consider the product $a(2a)(3a)\ldots((p-1)a) = (p-1)!a^{p-1}$. Let r_i be the remainder of ia when divided by p. Then the product above has the same remainder when divided by p as the product $r_1 r_2 \ldots r_{p-1}$. But this product is just $(p-1)!$. Hence p is a divisor of $(p-1)!a^{p-1} - (p-1)! = (p-1)!(a^{p-1} - 1)$. Since p is a prime, it is not a divisor of $(p-1)!$, and so it is a divisor of $a^{p-1} - 1$.

6.6 The Euclidean Algorithm

6.19. $\gcd(a, b) \leq a$, but a is a common divisor, so $\gcd(a, b) = a$.

6.20. (a) Let $d = \gcd(a, b)$. Then $d|a$ and $d|b$, and hence $d|b - a$. Thus d is a common divisor of a and $b - a$, and hence $d \leq \gcd(a, b)$. A similar argument show the reverse inequality. (b) By repeated application of (a).

6.21. (a) $\gcd(a/2, b)|(a/2)$ and hence $\gcd(a/2, b)|a$. So $\gcd(a/2, b)$ is a common divisor of a and b and hence $\gcd(a/2, b) \leq \gcd(a, b)$. The reverse inequality follows similarly, using that $\gcd(a, b)$ is odd, and hence $\gcd(a, b)|(a/2)$.
(b) $\gcd(a/2, b/2)|(a/2)$ and hence $2\gcd(a/2, b/2)|a$. Similarly, $2\gcd(a/2, b/2)|b$, and hence $2\gcd(a/2, b/2) \leq \gcd(a, b)$. Conversely, $\gcd(a, b)|a$ and hence $\frac{1}{2}\gcd(a, b)|a/2$. Similarly, $\frac{1}{2}\gcd(a, b)|b/2$, and hence $\frac{1}{2}\gcd(a, b) \leq \gcd(a/2, b/2)$.

6.22. Consider each prime that occurs in either one of them, raise it to the larger of the two exponents, and multiply these prime powers.

6.23. If a and b are the two integers, and you know the prime factorization of a, then take the prime factors of a one by one, divide b with them repeatedly to determine their exponent in the prime factorization of b, raise them to the smaller of their exponent in the prime factorizations of a and b, and multiply these prime powers.

6.24. By the descriptions of the gcd and lcm above, each prime occurs the same number of times in the prime factorization of both sides.

6.25. (a) Straightforward. (b) Let $z = \gcd(a, b, c)$, and let $A = a/z$, $B = b/z$, $C = c/z$. Then A, B and C are relatively prime and form a pythagorean triple. One of A and B must be odd, since if both of them were even, then so would C, and so they would not be relatively prime. Suppose that B is odd. Then A must be even. Indeed, the square of an odd number gives a remainder of 1 when divided by 4, so if both A and B were odd, then $C^2 = A^2 + B^2$ would give a remainder of 2 when divided by 4, which is impossible. It follows that C must be odd.
So A is even, and we can write it in the form $A = 2A_0$. Write the equation in the form

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

Let p be any prime number dividing A_0. Then p must divide either $(C + B)/2$ or $(C - B)/2$. But p cannot divide both, since then it would also divide the sum $\frac{C+B}{2} + \frac{C-B}{2} = C$ as well as the difference $\frac{C+B}{2} - \frac{C-B}{2} = B$, contradicting the assumption that A, B and C are relatively prime.
The prime p may occur in the prime decomposition of A_0 several times, say k times. Then in the prime decomposition of A_0^2, p occurs $2k$ times. By the argument above, p must occur $2k$ times in the prime decomposition of one of $(C + B)/2$ and $(C - B)/2$, and not at all in the prime decomposition of the other.
So we see that in the prime decomposition of $(C + B)/2$ (and similarly in the prime decomposition of $(C - B)/2$), every prime occurs with an even power. This is the same as saying that both $(C + B)/2$ and $(C - B)/2$ are squares: say, $(C + B)/2 = x^2$ and $(C - B)/2 = y^2$ for some integers x and y.
Now we can express A, B and C in terms of x and y:

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

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

We get a, b and c by multiplying A, B and C by z, which completes the solution.

6.26. $\gcd(a, a+1) = \gcd(a, 1) = \gcd(0, 1) = 1$.

6.27. The remainder of F_{n+1} divided by F_n is F_{n-1}. Hence $\gcd(F_{n+1}, F_n) = \gcd(F_n, F_{n-1}) = \ldots = \gcd(F_3, F_2) = 1$. This lasts $n-1$ steps.

6.28. By induction on k. True if $k = 1$. Suppose that $k > 1$. Let $b = aq + r$, $1 \le r < a$. Then the euclidean algorithm for computing $\gcd(a, r)$ lasts $k-1$ steps, hence $a \ge F_k$ and $r \ge F_{k-1}$ by the induction hypothesis. But then $b = aq + r \ge a + r \ge F_k + F_{k-1} = F_{k+1}$.

6.29. (a) Takes 10 steps. (b) Follows from $\gcd(a, b) = \gcd(a-b, b)$. (c) $\gcd(10^{100} - 1, 10^{100} - 2)$ takes $10^{100} - 1$ steps.

6.30. (a) Takes 8 steps. (b) At least one of the numbers remains odd all the time. (c) Follows from exercises 6.20 and 6.21. (d) The product of the two numbers drops by a factor of two in one of any two iterations.

6.7 Congruences

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

6.32. Only (b) is correct.

6.33. $a \equiv b \pmod 0$ should mean that there exists an integer k so that $a - b = 0 \cdot k$. This means that $a - b = 0$, or $a = b$. So equality can be considered as a special case of congruence.

6.34. (a) Take $a = 2$ and $b = 5$. (b) If $ac \equiv bc \pmod{mc}$ then $mc | ac - bc$, so there is an integer k such that $ac - bc = kmc$. Since $c \neq 0$, this implies that $a - b = km$, and so $a \equiv b \pmod m$.

6.35. First, from $x \equiv y \pmod p$ it follows (by the multiplication rule) that $x^v \equiv y^v \pmod p$, so it suffices to prove that

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

If $x \equiv 0 \pmod p$, then both sides of (16.1) are divisible by p, and the assertion follows. Suppose that $x \not\equiv 0 \pmod p$. Let, say, $u < v$. We know that $p - 1 | v - u$, so we can write $v - u = k(p-1)$ with some positive integer k. Now we know by Fermat's Little Theorem that $x^{p-1} \equiv 1 \pmod p$, hence by the multiplication rule of congruences, we have $x^{k(p-1)} \equiv 1 \pmod p$, and by the multiplication rule again, we get $x^v = x^u \cdot x^{k(p-1)} \equiv x^u \pmod p$, which proves (16.1).

6.8 Strange numbers

6.36. Tu; Sa; Th; We.

6.37. not-$A = 1 \oplus A$; A-or-$B = A \oplus B \oplus A \cdot B$; A-and-$B = A \cdot B$.

6.38. $2 \cdot 0 \equiv 2 \cdot 3 \pmod 6$ but $0 \not\equiv 3 \pmod 6$. More generally, if $m = ab$ $(a, b > 1)$ is a composite modulus, then $a \cdot 0 \equiv a \cdot b \pmod m$, but $0 \not\equiv b \pmod m$.

6.39. We start with the euclidean algorithm:

$$\gcd(53, 234527) = \gcd(53, 2) = \gcd(1, 2) = 1.$$

Here we got 2 as $2 = 234527 - 4425 \cdot 53$, and then 1 as

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

It follows that $1 \equiv 115051 \cdot 53 \pmod{234527}$, and so $\overline{1}/\overline{53} = \overline{115051}$.

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

6.41. (a) We have $11|x^2 - 2x = x(x-2)$, hence either $11|x$ or $11|x-2$, so $x \equiv 0 \pmod{11}$ and $x \equiv 2 \pmod{11}$ are the two solutions. (b) Similarly from $23|x^2-4 = (x-2)(x+2)$ we get $x \equiv 2 \pmod{23}$ or $x \equiv -2 \pmod{23}$.

6.9 Number theory and combinatorics

6.42. There are two neighboring integers k and $k+1$ among the given n numbers (Pigeon Hole Principle), which are relatively prime.

6.43. By the rules of inclusion-exclusion, we have to subtract from n the number of multiples of p_i (between 1 and n) for every p_i; then we have to add the number of common multiples of p_i and p_j for any two primes p_i and p_j; then we have to subtract the number of common multiples of p_i, p_j and p_k for any three primes p_i, p_j and p_k, etc. Just as in the numerical example, the number of multiples of p_i is n/p_i; the number of common multiples of p_i and p_j is $n/(p_ip_j)$; the number of common multiples of p_i, p_j and p_k is $n/(p_ip_jp_k)$, etc. So we get

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

This is equal to the expression in (6.7). Indeed, if we expand the product, every term arises by picking either "1" or "$-\frac{1}{p_i}$" from each factor "$\left(1 - \frac{1}{p_i}\right)$", which gives a term of the form

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

This is just a typical term in the inclusion-exclusion formula above.

6.44. It is not hard to come up with the conjecture that the answer is n. To prove this, consider the fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$, and simplify them as much as possible. We get fractions of the form $\frac{a}{d}$, where d is a divisor of n, $1 \le a \le d$, and $\gcd(a, d) = 1$. It is also clear that we get every such fraction. The number of such fractions with a given denominator is $\phi(d)$. Since the total number of fractions we started with is n, this proves our conjecture.

6.45. For $n = 1$ and 2 the answer is 1. Suppose that $n > 2$. If k is such an integer, then so is $n - k$. So these integers come in pairs adding up to n (we have to add that $n/2$ is not among these numbers). There are $\phi(n)/2$ such pairs, so the answer is $n\phi(n)/2$.

6.46. The proof is similar to the solution of exercise 6.18.
Let $s_1, \ldots, s_k$ be the numbers between 1 and b relatively prime to b; so $k = \phi(b)$. Let r_i be the remainder of $s_i a$ when divided by p. We have $\gcd(b, r_i) = 1$, since if there were

a prime p dividing both b and r_i, then p would also divide $s_i a$, which is impossible, since both s_i and a are relatively prime to b. Second, $r_1, r_2, \ldots, r_k$ are different, since $r_i = r_j$ would mean that $b|s_i a - s_j a = (s_i - s_j)a$; since $\gcd(a, b) = 1$, this would imply that $b|s_i - s_j$, which is clearly impossible. Hence it follows that $r_1, r_2, \ldots, r_k$ are just the numbers $s_1, s_2, \ldots, s_k$, in different order.
Consider the product $(s_1 a)(s_2 a) \ldots (s_k a)$. On the one hand we can write this as

$$(s_1 a)(s_2 a) \ldots (s_k a) = (s_1 s_2 \ldots s_k) a^k,$$

on the other,

$$(s_1 a)(s_2 a) \ldots (s_k a) \equiv r_1 r_2 \ldots r_k = s_1 s_2 \ldots s_k. \pmod{b}.$$

Comparing,

$$(s_1 s_2 \ldots s_k) a^k \equiv s_1 s_2 \ldots s_k \pmod{b},$$

or

$$b \mid (s_1 s_2 \ldots s_k)(a^k - 1)$$

Since $s_1 s_2 \ldots s_k$ is relatively prime to b, this implies that $b|a^k - 1$ as claimed.

6.10 How to test if a number is a prime?

6.47. By induction on k. True if $k = 1$. Let $n = 2m + a$, where a is 0 or 1. Then m has $k - 1$ bits, so by induction, we can compute 2^m using at most $2(k - 1)$ multiplications. Now $2^n = (2^m)^2$ if $a = 0$ and $2^n = (2^m)^2 \cdot 2$ if $a = 1$.

6.48. If $3|a$ then clearly $3|a^{561} - a$. If $3 \nmid a$, then $3|a^2 - 1$ by Fermat, hence $3|(a^2)^{280} - 1 = a^{560} - 1$. Similarly, if $11 \nmid a$, then $11|a^{10} - 1$ and hence $11|(a^{10})^{56} - 1 = a^{560} - 1$. Finally, if $17 \nmid a$, then $17|a^{16} - 1$ and hence $17|(a^{16})^{35} - 1 = a^{560} - 1$.

7 Graphs

7.1 Even and odd degrees

7.1. There are 2 graphs on 2 nodes, 8 graphs on 3 nodes (but only four "essentially different"), 64 graphs on 4 nodes (but only 11 "essentially different").

7.2. (a) No; the number of odd degrees must be even. (b) No; node with degree 5 must be connected to all other nodes, so we cannot have a node with degree 0. (c) 12 (but they are all "essentially the same"). (d) $9 \cdot 7 \cdot 5 \cdot 3 \cdot 1 = 945$ (but again they are all "essentially the same").

7.3. This graph, the *complete graph* has $\binom{n}{2}$ edges if it has n nodes.

7.4. In graph (a), the number of edges is 17, the degrees are $9, 5, 3, 3, 2, 3, 1, 3, 2, 3$. In graph (b), the number of edges is 31, the degrees are $9, 5, 7, 5, 8, 3, 9, 5, 7, 4$.

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

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

7.7. *Every graph has two nodes with the same degree.* Since each degree is between 0 and $n - 1$, if all degrees were different then they would be $0, 1, 2, 3, \ldots n - 1$ (in some

order). But the node with degree $n-1$ must be connected to all the others, in particular to the node with degree 0, which is impossible.

7.2 Paths, cycles, and connectivity

7.8. There are 4 paths, 6 cycles and 1 complete graph.

7.9. The empty graph on n nodes has 2^n subgraphs. The triangle has 18 subgraphs.

7.10. The path of length 3 and the cycle of length 5 are the only examples. (The complement of a longer path or cycle has too many edges.)

7.11. Yes, the proof remains valid.

7.12. (a) Delete any edge from a path. (b) Consider two nodes u and v. the original graph contains a path connecting them. If this does not go through e, then it remains a path after e is deleted. If it goes through e, then let $e = xy$, and assume that the path reaches x first (when traversed from u to v). Then after e is deleted, there is a path in the remaining graph from u to x, and also from x to y (the remainder of the cycle), so there is one from u to y. but there is also one from y to v, so there is also a path from u to v.

7.13. (a) Consider a shortest walk from u to v; if this goes through any nodes more than once, the part of it between two passes through this node can be deleted, to make it shorter. (b) The two paths together form a walk from a to c.

7.14. Let w be a common node of H_1 and H_2. If you want a path between nodes u and v in H, then we can take a path from u to w, followed by a path from w to v, to get a walk from u to w.

7.15. Both graphs are connected.

7.16. The union of this edge and one of these components would form a connected graph that is strictly larger than the component, contradicting the definition of a component.

7.17. If u and v are in the same connected component, then this component, and hence G too, contains a path connecting them. Conversely, if there is a path P in G connecting u and v, then this path is a connected subgraph, and a maximal connected subgraph containing P is a connected component containing u and v.

7.18. Assume that the graph is not connected and let a connected component H of it have k nodes. Then H has at most $\binom{k}{2}$ edges. The rest of the graph has at most $\binom{n-k}{2}$ edges. Then the number of edges is at most

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

7.14 Eulerian walks and Hamiltonian cycles

7.19. The upper left graph does not have an Eulerian walk. The lower left graph has an open Eulerian walk. The two graphs on the right have closed Eulerian walks.

7.20. Every node with an odd degree must be the an endpoint of one of the two walks, so a necessary condition is that the number of nodes with odd degree is at most four.

We show that this condition is also sufficient. We know that the number of nodes with odd degree is even. If this number is 0 or 2, then there is a single Eulerian walk (and we can take any single node as the other walk).
Suppose that this number is four. Add a new edge, connecting two of the nodes with odd degree. Then there are only two nodes with odd degree left, so the graph has an Eulerian walk. deleting the edge splits this walk into two, which together use every edge exactly once.

7.21. The first graph does; the second does not.

8 Trees

8.1 How to define a tree?

8.1. If G is a tree then it contains no cycles (by definition), but adding any new edge creates a cycle (with the path in the tree connecting the endpoints of the new edge). Conversely, if a graph has no cycles but adding any edge creates a cycle, then it is connected (two nodes u and v are either connected by an edge, or else adding an edge connecting them creates a cycle, which contains a path between u and v in the old graph), and therefore it is a tree.

8.2. If u and v are in the same connected component, then the new edge uv forms a cycle with the path connecting u and v in the old graph. If joining u and v by a new edge creates a cycle, then the rest of this cycle is path between u and v, and hence u and v are in the same component.

8.3. Assume that G is a tree. Then there is at least one path between two nodes, by connectivity. But there cannot be two paths, since then we would get a cycle (find the node v when the two paths branch away, and follow the second path until it hits the first path again; follow the first path back to v, to get a cycle).
Conversely, assume that there is a unique path between each pair of nodes. Then the graph is connected (since there is a path) and cannot contain a cycle (since two nodes on the cycle would have at least two paths connecting them).

8.2 How to grow a tree?

8.4. Start the path from a node of degree 1.

8.5. Any edge has only one lord, since if there were two, they would have to start from different ends, and they would have then two ways to get to the King: either continuing as they started, or waiting for the other and walk together. Similarly, an edge with no lord would have to lead to two different ways of walking.

8.6. Start at any node v. If one of the branches at this node contains more than half of all nodes, move along the edge leading to this branch. Repeat. You'll never backtrack because this would mean that there is an edge whose deletion results in two connected components, both containing more than half of the nodes. You'll never cycle back to a node already seen because the graph is a tree. Therefore you must get stuck at a node such that each branch at this node contains at most half of all nodes.

8.3 How to count trees?

8.7. The number of unlabeled trees on $2, 3, 4, 5$ nodes is $1, 1, 2, 3$. They give rise to a total of $1, 3, 16, 125$ labeled trees.

8.8. There are n stars and $n!/2$ paths on n nodes.

8.4 How to store a tree?

8.9. The first is the father code of a path; the third is the father code of a star. The other two are not father codes of trees.

8.10. This is the number of possible father codes.

8.11. Define a graph on $\{1, \ldots, n\}$ by connecting all pairs of nodes in the same column. If we do it backwards, starting with the last column, we get a procedure of growing a tree by adding new node and an edge connecting it to an old node.

8.12. (a) encodes a path; (b) encodes a star; (c) does not encode any tree (there are more 0's than 1's among the first 5 elements, which is impossible in the planar code of any tree).

9 Finding the optimum

9.1 Finding the best tree

9.1. Let H be an optimal tree and let G be the tree constructed by the pessimistic government. Look at the first step when an edge $e = uv$ of H is eliminated. Deleting e from H we get two components; since G is connected, it has an edge f connecting these two components. The edge f cannot be more expensive than e, else the pessimistic government would have chosen f to eliminate instead of e. But then we can replace e by f in H without increasing its cost. Hence we conclude as in the proof given above.

9.2. [Very similar.]

9.3. [Very similar.]

9.4. Take nodes $1, 2, 3, 4$ and costs $c(12) = c(23) = c(34) = c(41) = 3$, $c(13) = 4$, $c(24) = 1$. The pessimistic government builds (12341), while the best solution is 12431.

9.2 Traveling Salesman

9.5. No, because it intersects itself (see next exercise).

9.6. Replacing two intersecting edges by two other edges pairing up the same 4 nodes, just differently, gives a shorter tour by the triangle inequality.

10 Matchings in graphs

10.1 A dancing problem

10.1. If every degree is d, then the number of edges is $d \cdot |A|$, but also $d \cdot |B|$.

10.2. (a) A triangle; (b) a star.

10.3. A graph in which every node has degree 2 is the union of disjoint cycles. If the graph is bipartite, these cycles have even length.

10.3 The main theorem

10.4. Let $X \subseteq A$ and let Y denote the set of neighbors of X in B. There are exactly $d|X|$ edges starting from X. Every node in Y accommodates no more than d of these; hence $|Y| \geq |X|$.

10.5. The assumption for $X = A$ yields that $|B| \geq |A|$. If $|B| = |A|$ then we already know the assertion (Theorem 10.3.1), so suppose that $|B| > |A|$. Add $|B| - |A|$ new nodes to A, to get a set A' with $|A'| = |B|$. Connect every new node to every node in B. The graph we get satisfies the conditions in the Marriage Theorem 10.3.1: we have $|A'| = |B|$, and if $X \subseteq A'$ then either $X \subseteq A$ (in which case it has at least $|X|$ neighbors in B by the assumption of the exercise), or X contains a new node, in which case every node in B is a neighbor of X. So the new graph has a perfect matching. Deleting the newly added nodes, the edges of the perfect matching that remain match all nodes of A with different nodes of B.

10.4 How to find a perfect matching?

10.6. On a path with 4 nodes, we may select the middle edge.

10.7. The edges in the greedy matching M must meet every edge in G (otherwise, we could further extend M), in particular every edge in the perfect matching matching. So every edge in the perfect matching has at most one endpoint unmatched by M.

10.8. The largest matching has 5 edges.

10.9. If the algorithm terminates without a perfect matching, then the set S shows that the graph is not "good".

11 Combinatorics in Geometry

11.1 Intersections of diagonals

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

11.2 Counting regions

11.2. True for $n = 1$. Let $n > 1$. Delete any line. The remaining lines divide the plane into $(n-1)n/2 + 1$ regions by the induction hypothesis. The last line cuts n of these into two. So we get

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

11.3 Convex polygons

11.3. See Figure 16.1.

12 Euler's Formula

12.1 A planet under attack

12.1. There are n nodes of degree $n-1$ and $\binom{n}{4}$ nodes of degree 4 (see section 11.1). So the number of edges is $\frac{1}{2}\left(n \cdot (n-1) + \binom{n}{4} \cdot 4\right)$. From Euler's Formula, the number of countries is

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

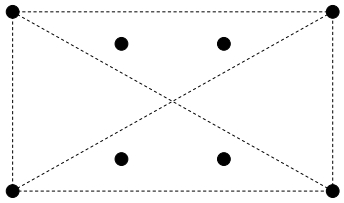

Figura 16.1:

you have to subtract 1 for the country outside.

12.2. Let f be the number of regions of the island. Consider the graph formed by the dams and also the boundary of the island. There are $2n$ nodes of degree 3 (along the shore), and $\binom{n}{2}$ nodes of degree 4 (the intersection points of straight dams). So the number of edges is

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

The number of countries is $f+1$ (we have to count the ocean too), so Euler's formula gives $f+1+2n+\binom{n}{2}=2\binom{n}{2}+3n+2$, whence $f=\binom{n}{2}+n+1$.

12.2 Planar graphs

12.3. Yes, s

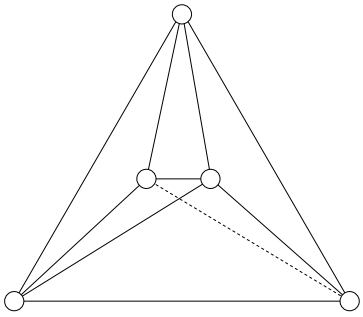

Figura 16.2:

12.4. No; the argument is similar to the one showing that K_5 is not planar. The houses, wells and paths form a bipartite graph with 6 nodes and 9 edges. Suppose that this can be drawn in the plane without intersections. Then we have $9+2-6=5$ regions. Each region has at least 4 edges (since there are no triangles), and hence the number of edges is at least $\frac{1}{2}\cdot 5\cdot 4=10$, which is a contradiction.

13 Coloring maps and graphs

13.1 Coloring regions: a simple case

13.1. By induction. True if $n = 1$. Let $n > 1$. Assume the description of the coloring is valid for the first $n - 1$ circles. If we add the n-th, the color and the parity don't change outside this circle; both change inside the circle. So the description remains valid.

13.2. (a) By induction. True for 1 line. Adding a line, we re-color all regions on one side.
(b) One possible description: designate a direction as "up". Let p any point not on any of the lines. Start a semiline "up" from P. Count how many of the given lines intersect it. Color according to the parity of this intersection number.

13.1 Coloring graphs with two colors

13.3. This graph can not contain any odd cycle. Indeed, if we consider any cycle C, then each edge of it contains exactly one intersection point with the union of circles. The contribution of every circle is even, since walking around C, we cross the circle alternatingly in and out.

13.3 Coloring graphs with many colors

13.4. Suppose that we have a good 3-coloring of the first graph. Starting from above, the first vertex gets (say) color 1, the vertices on the second level must get colors 2 and 3, and then both of the lowest two vertices must get color 1. But this is impossible, since they are connected.
Suppose that we have a good 3-coloring of the second graph. Starting from the center, we may assume that it has color 1, so its neighbors get colors 2 or 3. Now recolor each outermost vertex with color 1 by giving it the color of their inner "twin". This coloring would give a good coloring of a 5-cycle by 2 colors, since "twins" have the same neighbors (except that the inner twin is also connected to the center). This is a contradiction.

13.5. By rotating the plane a little, we may assume that all intersection points have different y coordinates (which we just call "heights"). Starting with the highest intersection point, and moving down, we can color the intersection points one by one. Each time there are at most two intersection points that are adjacent to the current point along the two lines which were colored previously, and so we can find a color for the current point different from these.

13.6. We may assume that there are at least 2 nodes, and so there is a node of degree at most d. We delete it, recursively color the remaining graph by $d + 1$ colors, and then we can extend this coloring to the last point, since its d neighbors exclude only d colors.

13.7. We delete a point of degree d, and recursively color the remaining graph with $d + 1$ colors. We can extend this as in the previous solution.

13.4 Map coloring and the Four Color Theorem

14 Finite geometries, codes, Latin squares, and other pretty creatures

14.1 Small exotic worlds

14.1. The Fano plane itself.

14.2. Let abc be a circle. Then two of the lines through a contain b and c, respectively, so they are not tangents. The third line through a is the tangent.

14.3. If H is a hypercircle, then its 4 points determine 6 lines, and 3 of these 6 lines go through each of its points. So the 7th line does not go through any of the 4 points of the hypercircle. Conversely, if L is a line, then the 4 points not on L cannot contain another line (else, these two lines would not intersect), and so these 4 points form a hypercircle.

14.4. (a) If everybody on line L votes YES, then (since every line intersects L) every line has at least one point voting YES, and so no line will vote all-NO. (b) We may assume that at least 4 points vote YES; let a, b, c and d be 4 of them. Suppose that there is no line voting all-YES. Then each of the 3 lines through a contain at most one further YES vote, so each of them must contain exactly one of b, c and d. So the remaining 3 points vote NO. The YES votes form a hypercircle (exercise 14.3), so the NO votes form a line.

14.5. (a) Through two original points, there is the original line; through an original point a and a new point b, there is a unique line through a among all parallel lines to which b was added; and for two new points, there is the new line. (b) is similar. (c) is obvious. (d) follows from (a)-(b)-(c), as we saw above.

14.6. Yes: for every line (2 points) there is exactly one line that is disjoint from it (the other 2 points).

14.7. See Figure 16.3 (there are many other ways to map the points)

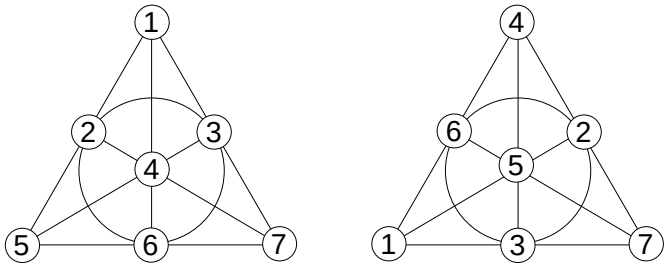

Figura 16.3:

14.8. This is not a coincidence. Fix any point A of the Cube space. Every plane through A contains 3 lines through A. If we call the lines through a given point "POINTS", and those triples of these lines that belong to one plane "LINES", then these POINTS and LINES form a Fano plane.

14.2 Finite affine and projective planes

14.9. Fix any point a. There are $n+1$ lines through a, which have no other points in common and cover the whole plane by (a). Each of these lines has n points besides a, so there are $(n+1)n$ points besides a, and $n(n+1)+1 = n^2+n+1$ points altogether.

14.10. We can assign coordinates to the vertices of the cube as if it were in the euclidean space, but think of the coordinates as elements of the 2-element field (Figure 16.4). Then it is straightforward (if lengthy) to check that the planes of the Cube space are precisely the sets of points given by linear equations. For example, the linear equation $x + y + z = 1$ gives the points $001,\ 010,\ 011,\ 111$ (don't forget, we are working in the 2-element field), which is just the plane consisting of the light points.

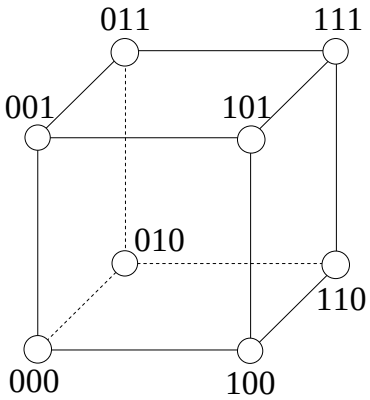

Figura 16.4:

14.11. A projective plane of order 10 ought to have $10^2 + 10 + 1 = 111$ points, 111 lines, with 11 points on each line. The number of ways to select a candidate line is $\binom{111}{11}$; the number of ways to select 111 candidate lines is

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

One could not check so many possibilities even with the fastest computer within the lifetime of the universe! Lam, Thiel and Swiercz had to work in a much more sophisticated manner.

14.3 Block designs

14.12. 441, 44.

14.13. For any two citizens C and D, there are λ clubs containing both. If we add this up for every D, we count $(v-1)\lambda$ clubs containing C. Each such club is counted $k-1$ times (once for every member different from C, so the number of clubs containing C is $(v-1)\lambda/k$. This is the same for every citizen C.

14.14. (a) $v = 6$, $r = 3$, $k = 3$ gives $b = 6$ by (14.1), but $\lambda = 6/5$ by (14.2). (b) $b = 8$, $v = 16$, $r = 3$, $k = 6$, $\lambda = 1$ (there are many other examples in both cases).

14.15. Take $b = v$ clubs, and construct for every citizen C a club in which everybody else is a member except C. Then $b = v$, $k = v - 1$, $r = v - 1$, $\lambda = v - 2$.

14.4 Steiner systems

14.16. Let A, B, C be 3 elements that do not form a club. There is a unique club containing A and B, which has a unique third element; call this D. Similarly, there is a unique element E such that ACE is a club, and a unique element F such that BCF is a club. The elements D, E, F must be distinct, since if (say) $D = E$, then A and D are contained in two clubs (one with B and one with C). Let the 7th element be G. There is a unique club containing C and D, and the third member of this club must be G (we can check that any of the other 4 choices would yield two clubs with two members is common). Similarly, AFG and BEG are clubs. Similarly, there is a unique club containing D and E, whose third member must be F. So, apart from the names of the citizens, the club structure is uniquely determined.

14.17. We have $r = (v-1)/2$ by (14.2), and hence $b = v(v-1)/6$ by (14.1). Since $v - 1 \geq 6$, we have $b \geq v$.

14.18. Call a triple contained in S and S-triple. The total number of triples is $b = v(v-1)/6$, the number of S-triples is

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

and so the number of non-S-triples is $b - b' = \frac{(v+1)(v-1)}{8}$. Every non-$S$-triple has at most one point in S and thus at least two points not in S. But the number of pairs not is S is $\binom{(v+1)/2}{2} = \frac{(v+1)(v-1)}{8}$, an since these pairs can belong to one of the non-S-triples only, it follows that each of the non-S-triples must contain exactly one pair of elements outside S. This proves that each non-S-triple must contain an element of S.

14.19. See Figure 16.5.

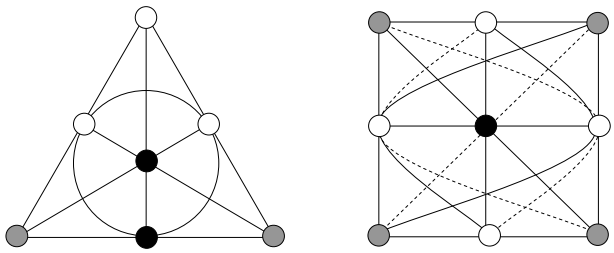

Figura 16.5:

14.20. Every girl has 8 other girls to walk with, every day she can walk with 2 in a line. So 4 days are necessary for her to walk with everybody exactly once.

14.5 Latin squares

14.21. There are 576 different 4×4 Latin squares. There are many ways to arrive at this figure; we sketch one. The first row can be filled out 4! ways. These are all equivalent in the sense that the number of ways they can be completed is the same for each of them, so we may fix the first row as 0 1 2 3 and just count the number of ways to complete this. The first column now can be filled out in 3! ways, and again all of these are equivalent, so let's fix it as 0 1 2 3.

If the 0 in the second row is in the second position, then the rest of the second row and second column is forced, but we get two ways to fill out the 4 fields in the lower right corner. If the 0 in the second row is in the third or fourth position, then the way to fill out the rest is forced. Thus we get the 4 Latin squares below:

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

Therefore the number of ways to fill out the remaining 9 fields is 4, so the total number is $4! \cdot 3! \cdot 4 = 576$.

These four may look different, but if we flip 1 and 2 in the third, flip rows 2 and 3, and flip columns 2 and 3, we get the second. Similarly, if we flip 1 and 3 in the fourth, flip rows 2 and 4, and flip columns 2 and 4, we get the second. So the last 3 of these are not essentially different.

There is no way to get the second square from the first by such operations (this follows e.g. by exercise 14.27). So there are two essentially different 4×4 Latin squares.

14.22. This is quite simple. For example, the table below is good (there are many other possibilities):

0	1	2	...	n-2	n-1
1	2	3	...	n-1	0
2	3	4	...	0	1
⋮					⋮
n-1	0	1	...	n-3	n-2

14.23.

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

14.24. We add 1 to every number, this way every row and column sum increases by 4.

14.25. We need two Latin squares where not only in the rows and columns, but also in the diagonals every number occurs once. These two will do:

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

From these two we get the following perfect magic square:

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

14.26. If there exists such a Latin square, then arbitrarily permuting the numbers 0,1,2,3 in it would give another square orthogonal to the three squares in (14.9) and

(14.12). (Prove!) So we may start with a square having its first row 0 1 2 3. But then what can be its first entry in the second row? 0 is impossible (because the entry above it is also 0), but 1, 2 or 3 are also ruled out: for instance if we had 2, then it wouldn't be orthogonal to square (14.12), because the pair (2,2) would occur twice. So there does not exist such a Latin square. (Try to generalize this result: from the $n \times n$ Latin squares, we can choose at most $n - 1$ squares pairwise orthogonal to each other.)

14.27. If we had a square orthogonal to (14.13), then using the same argument as in the solution of exercise 14.26, we may suppose that the first row is 0 1 2 3. Then the pairs (0,0), (1,1), (2,2) and (3,3) occur in the first row, which implies that in the other rows, the two squares cannot have the same number in the same position.
In particular, the first entry of the second row cannot be 1, and it cannot be 0 (because the entry above it is 0). So it is 2 or 3.
Suppose it is 2. Then the second entry in this row cannot be 1 or 2 (there is a 1 above it and a 2 before it), and it cannot be 3, so it is 0. The 4th entry cannot be 2,0 or 3, so it must be 1; it follows that the second row is 2 0 3 1 (same as the third row in (14.13)). Next we can figure out the last row: each entry is different from the two above it in the first and second row, and also from the last row of (14.13), which implies that this row must be the same as the second row of (14.13): 1 3 0 2. Hence the third row must be 3 2 1 0; but now the pair (3,1) occurs twice when the last two rows are overlaid.
The case when the second row starts with a 3 can be argued in the same way.

14.6 Codes

14.28. Suppose that a code is d-error-correcting. We claim that for any two codewords, we must flip at least $2d + 1$ bits to get from one to the other. Indeed, if we could get from codeword u to codeword v by flipping only $2d$ bits, then consider the codeword w obtained from u by flipping d of these bits. We could receive w instead of u, , but also instead of v, so the code is not d-error-correcting.
Now if we receive any message which has at most $2d$ errors, then this message is not another codeword, so we can detect up to $2d$ errors.
The converse is proved similarly.

14.29. If the string has no 1's, then it is a codeword. If it contains one 1, this can be flipped to get a codeword. If it has two 1's, then there is a line through the corresponding two points of the Fano plane, and flipping the 0 in the position corresponding to the third point gives a codeword. If it has three 1's, and these are collinear, then it is a codeword. If it has three 1's, and these are not collinear, then there is a unique point not on any of the three lines determined by them, and flipping this we get a codeword. If it contains at least four 1's, then we can argue similarly, interchanging the role of 1's and 0's.

15 A glimpse of complexity and cryptography

15.2 Classical cryptography

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

15.2. Let $a_1 a_2 \dots a_n$ be the key and $b_1 b_2 \dots b_n$, the plain text. Caligula intercepts one message whose bits are $a_2 \oplus b_1$, $a_3 \oplus b_2$, $\dots$ $a_n \oplus b_{n-1}$, and another message whose bits

are $a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n$. (The second message is one bit longer, which may give him a hint of what happened.) He can compute the binary sum of the first bits, second bits, etc. So he gets $(a_2 \oplus b_1) \oplus (a_1 \oplus b_1) = a_1 \oplus a_2$, $(a_3 \oplus b_2) \oplus (a_2 \oplus b_2) = a_2 \oplus a_3$, etc.
Now he guesses that $a_1 = 0$; since he knows $a_1 \oplus a_2$, he can compute a_2, then similarly a_3, and so on, he gets the whole key. It may be that his initial guess was wrong, which he notices since trying to decode the message he gets garbage; but then he can try out $a_1 = 1$, and recover the key. One of the two guesses will work.

15.3. Let $a_1 a_2 \ldots a_n$ be the key and let $b_1 b_2 \ldots b_n$ and $c_1 c_2 \ldots c_n$ be the two plain texts. Caligula intercepts one message whose bits are $a_1 \oplus b_1, a_2 \oplus b_2, \ldots a_n \oplus b_n$, and another message whose bits are $a_1 \oplus c_1, a_2 \oplus c_2, \ldots, a_n \oplus c_n$. As before, he computes the binary sum of the first bits, second bits, etc., to get $(a_1 \oplus b_1) \oplus (a_1 \oplus c_1) = b_1 \oplus c_1$, $(a_2 \oplus b_2) \oplus (a_2 \oplus c_2) = b_2 \oplus c_2$, etc.
The rest is not as straightforward as in the previous exercise, but suppose that Caligula can guess part of (say) Arthur's message (signature, or address, or the like). Then, since he knows the bit-by-bit binary sum of the two messages, he can recover the corresponding part of Bela's message. With luck, this is not a full phrase, and it contains part of a word. Then he can guess the rest of the word, and this gives him a few more letters of Arthur's message. With luck, this suggests some more letters Bela's message etc.
This is not completely straightforward, but typically it gives enough information to decode the messages (as World War II codebreakers learned it). One important point: Caligula can *verify* that his reconstruction is correct, since in this case both messages must turn out meaningful.

15.3 How to save the last move in chess?

15.4. Alice can easily cheat: she can send just a random string x in the evening, figure out her move overnight, along with the string y that encodes it, and send the binary sum of x and y as the alleged key.

15.5. This certainly eliminates the cheating in the previous exercise, since if she changes her mind, the "key" she computes back from the message the next morning will not be meaningful. But now Bob has the advantage: he can try out all "random but meaningful" keys, since there are not so many of them.

15.6 Public key cryptography

15.6. (a) Pick randomly numbers (public keys) $e_1, e_2, \ldots e_M$ and apply the hypothesized algorithm to compute the the corresponding secret keys $d_1, d_2, \ldots, d_M$. The number $k = (p-1)(q-1)$ is a common divisor of $e_1 d_1 - 1, e_2 d_2 - 1, \ldots, e_M d_M - 1$, so it is a divisor of $K = \gcd(e_1 d_1 - 1, e_2 d_2 - 1, \ldots, e_M d_M - 1)$, which we can compute. If $K < m$, then we know that in fact $k = K$, since $k = (p-1)(q-1) > pq/2 = m/2$. Else we pick another public key e_{M+1} and repeat. One can show that after no more than about $\log m$ iterations, we find k with large probability.
(b) If we know $m = pq$ and $k = (p-1)(q-1)$, then we know $p + q = m - k + 1$, and so p and q can be determined as the solutions of the quadratic equation $x^2 - (m - k + 1)x + m = 0$.