12. **Only one cake.** Because there are more people than possible birthdays, there must be at least two people that share the same birthday. To be more convincing, imagine that they all have different birthdays. Now select 366 people from the group. Because they all have different birthdays and because there are only 366 possible birthdays (including leap year), all the birthdays must be accounted for. The remaining four people must all share a birthday with someone else in the room.

13. **For the birds.** There must be some hole containing more than one pigeon. In the hairy-bodies question, the six billion people in the world play the role of the pigeons, and the 400 million hairs play the role of the holes. Just as there are at least two pigeons sleeping in the same hole, there are necessarily two people with the same total number of body hairs.

14. **Sock hop.** To guarantee one match, you need only pull out three socks. Either two will be black, or two will be blue. To get two matched pairs, you need at most seven socks. However, to guarantee a black pair, you need to pull out 12 socks, because you might be unlucky and pull out all the blue socks first!

15. **The last one.** 19, 58, 29, 88, 44, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1. The sequences for 11 and 22 are within the sequence above.
30, 15, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1

Creating New Ideas

16. **See the three.** There are two ways to approach this question: (1) Count the numbers with 3's or (2) count the numbers without 3's. Method (1): There is only one number with three 3's in it, namely 333. How many numbers have exactly two 3's? There are 9 such numbers of the form 33*x*, 9 of the form 3*x*3, and 9 of the form *x*33, for a total of 27 "doubles". How many numbers have exactly one 3 in them? Let's overcount by saying that there are 100 numbers of the form *xx*3, *x*3*x*, and 3*xx*. Of the 300 numbers, we counted the 27 doubles twice, and 333 three times. So we have $300 - 27 - 2 = 271$. The corresponding proportion is 0.271. Method (2): A number with no 3 could have any of 9 digits in each position, for a total of $9 \times 9 \times 9$, or 729 numbers. The remaining 271 numbers have a 3.

17. **See the three II.** There are two ways to approach this question: (1) Count the numbers with 3's or (2) Count the numbers without 3's. Method (1): There is a nonobvious way to keep track of all the overcounting. There are 1000 numbers of the forms *xxx*3, *xx*3*x*, *x*3*xx*, and 3*xxx*, for a total of 4000. There are 100 numbers of the form *xx*33, *x*3*x*3, 3*xx*3, *x*33*x*, 3*x*3*x*, and 33*xx*, for a total of 600. We have 10 each of the form *x*333, 3*x*33, 33*x*3, and 333*x* for a total of 40 such numbers. And lastly, there is only 1 number with four 3's. Here's the trick: $4000 - 600 + 40 - 1 = 3439$ represents the number of numbers with 3's in them. The alternating signs account for all the overcounting! The corresponding proportion is 0.3439. Method (2): A number with no 3 could have any of 9 digits in each position, for a total of $9 \times 9 \times 9 \times 9$ or 6,561 numbers. The remaining 3,439 numbers have a 3.

18. **See the three III.** The proportion of million-digit numbers without a 3 is (9/10) raised to the millionth power.

19. **Commuting.** There are 100 people arriving at work between 8:00 and 8:30. Imagine slicing this time frame into 30 distinct intervals. Because we have more people than intervals, at least two people will arrive within the same interval. This also means that their arrival times differ by less than a minute.

20. **RIP.** Within the next 100 years, virtually all of the 6.2 billion people currently populating the earth will die. If fewer than 50 million people died each year, then at the end of 100 years, only 5 billion people would have died, which means that well over 100 billion people would live to at least 100. This contradiction shows that at some point more than 50 million people will die. Alternatively, you could say that the average number of people that will die each year is 6,200,000,000 / 100, or 62

2.2. Numerical Patterns in Nature

Developing Ideas

1. First Fibonaccis. 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610.

2. Born φ. The symbol φ represents the infinitely long fraction expression $1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ddots}}}$.

It is also a solution to the equation $\varphi = 1+\dfrac{1}{\varphi}$.

One sequence of numbers that approaches φ is the list of ratios of consecutive Fibonacci numbers.

3. Tons of ones. Simplifying, we see that $1+\dfrac{1}{1+\dfrac{1}{1}} = 1+\dfrac{1}{1+1} = \dfrac{3}{2}$.

4. Twos and threes. $2+\dfrac{2}{2+\dfrac{2}{2}} = 2+\dfrac{2}{2+1} = \dfrac{8}{3}$; $3+\dfrac{3}{3+\dfrac{3}{3}} = 3+\dfrac{3}{4} = \dfrac{15}{4}$.

5. The family of φ. If $x = 2+\dfrac{1}{x}$, multiply through by x to get $x^2 = 2x + 1$. So $x^2 - 2x - 1 = 0$. This does not factor, so we use the quadratic formula to get $x = \dfrac{-(-2) \pm \sqrt{(-2)^2 - 4(1)(-1)}}{2(1)} = \dfrac{2 \pm \sqrt{8}}{2} = 1 \pm \sqrt{2}$. Similarly, multiply $x = 3+\dfrac{1}{x}$ through by x to get $x^2 = 3x + 1$. So $x^2 - 3x - 1 = 0$. Again this does not factor, so we use the quadratic formula to get $x = \dfrac{-(-3) \pm \sqrt{(-3)^2 - 4(1)(-1)}}{2(1)} = \dfrac{2 \pm \sqrt{13}}{2}$.

Solidifying Ideas

6. Baby bunnies.

Month		1	2	3	4	5	6	7	8
Pairs of adults	1	1	2	3	5	8	13	21	
Pairs of babies	0	1	1	2	3	5	8	13	
Total number of pairs	1	2	3	5	8	13	21	34	

After each month, the total number of pairs of bunnies becomes the number of mature pairs for the next month. Because all the mature pairs produce offspring, the number of mature pairs during one month becomes the number of new pairs of offspring in the next month. Each row contains the same sequence of numbers, but the sequences are offset from one another. Note the connection to Fibonacci.

7. Discovering Fibonacci relationships.

n		1	2	3	4	5	6	
$(F_n)^2$		1	1	4	9	25	64	…
$(F_{n+1})^2$	1	4	9	25	64	169	…	
Sum		2	5	13	34	89	233	
		F_3	F_5	F_7	F_9	F_{11}	F_{13}	

Note that we are getting all the odd Fibonacci numbers. This leads to the formula, $(F_n)^2 + (F_{n+1})^2 = F_{2n+1}$.

8. Discovering more Fibonacci relationships.

n		1	2	3	4	5	6
$(F_{n+1})^2$	1	4	9	25	64	169	…
$(F_{n-1})^2$	.	1	1	4	9	25	…
Difference		.	3	8	21	55	144
			F_4	F_6	F_8	F_{10}	F_{12}

Now we're getting all the even Fibonacci numbers (see Mindscape 7.). More compactly, $(F_{n+1})^2 - (F_{n-1})^2 = F_{2n}$

9. Late bloomers.

Month	2	3	4	5	6	7	8	9	10	11
Mature pairs	1	1	1	2	3	4	6	9	13	19
Pairs of new babies	0	1	1	1	2	3	4	6	9	13
Pairs of old babies	0	0	1	1	1	2	3	4	6	9
Total pairs	1	2	3	4	6	9	13	19	28	41

As in Mindscape 6, starting with Month 2, each row contains the same sequence of numbers (though shifted). If T_n represents the total number of pairs of bunnies at the end of the nth month, then $T_n = T_{n-1} + T_{n-3}$.

10. A new Start. 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843,… Because 843/521 = 1.61803…, it looks like the ratio of consecutive numbers still approaches the golden mean.

If we start with – 7 and 3, we get a sequence that includes negative numbers:
– 7, 3, – 4, – 1, – 5, – 6, – 11, – 17, – 28, – 45, – 73, – 118, – 191, 309, – 500,… Yet the ratios still converge to the Golden Mean, (– 500)/(– 309) = 1.61812… We can view the Golden Mean as defined by this infinite process independent of the starting numbers. In Chapter 6, we will see that images and pictures can be defined in a similar manner.

11. Discovering Lucas relationships.

n		1	2	3	4	5	6	7	8
$L(n-1)$	.	2	1	3	4	7	11	18	
$L(n+1)$	1	3	4	7	11	18	29	47	
Sum		.	5	5	10	15	25	40	65
			g_1	g_2	g_3	g_4	g_5	g_6	g_7

$L_{(n-1)} + L_{(n+1)} = g_{(n-1)}$, where g_n's are constructed as the Lucas numbers are, but with the first two numbers being 5 and 5 instead of 2 and 1. You can write the answer in terms of Fibonacci numbers by noting that $L_n = F_n + F_{(n-2)}$.

12. Still more Fibonacci relationships.

See the solution to Mindscape 11. By the same reasoning, we find that the sum is the Lucas sequence starting with 3 and 4.

$F_{(n-1)}$	.	1	1	2	3	5	8	13	21
$F_{(n+1)}$	1	2	3	5	8	13	21	34	55
Sum	.	3	4	7	11	18	29	47	76

13. Even more Fibonacci relationships.

$F_{(n+2)}$	2	3	5	8	13	21	34
$F_{(n-2)}$	.	.	1	1	2	3	5
Difference	.	.	4	7	11	18	29

Note that we get the same sequence as in Mindscape 12. This is because $F_{(n+2)} - F_{(n-2)} = F_{(n-1)} + F_{(n+1)}$, which is straightforward to prove using the definition of Fibonacci numbers.

14. Discovering Fibonacci and Lucas relationships.

N	1	2	3	4	5	6	7	8
F_n	1	1	2	3	5	8	13	21
L_n	2	1	3	4	7	11	18	…
Sum	3	2	5	7	12	19	31	…

See Mindscape 11 for more insights into these types of sequences.

15. The enlarging area paradox. If you look closely, you'll notice that the pieces don't line up exactly. Note that the little triangle with sides 3 and 8 appears to be similar to the big "triangle" with sides 5 and 13. If this were true, then the corresponding ratios would be equal. But 8/3 isn't 13/5. Because these are ratios of consecutive Fibonacci numbers, the ratios are close, which is why this is a convincing trick.

16. Sum of Fibonacci. Start with the largest Fibonacci number smaller than the given number and work your way backwards

52 = 34 + 13 + 5,
143 = 89 + 34 + 13 + 5 + 2
13 = 13,
88 = 55 + 21 + 8 + 3 + 1

17. Some more sums. 43 = 34 + 8 + 1; 90 = 89 + 1; 2000 = 1597 + 377 + 21 + 5; 609 = 377 + 144 + 55 + 21 + 8 + 3 + 1

18. Fibonacci nim: The first move. After mentally expressing 52 as a sum of non-consecutive Fibonacci numbers, (52 = 34 + 13 + 5), you remove five sticks from the pile.

19. Fibonacci nim: The first move II. Because 100 = 89 + 8 + 3, you need only remove three sticks.

20. Fibonacci nim: The first move III. Noting that 609 = 377 + 144 + 55 + 21 + 8 + 3 + 1, we remove only one stick.

21. Fibonacci nim: The next move. After the friend removes four, there are nine sticks left. Because 9 = 8 + 1, so we remove one stick to keep ourselves in a winning position.

22. Fibonacci nim: The next move II. A total of 26 sticks have been removed, leaving 24. Express 24 as a sum of non-consecutive Fibonacci numbers (24 = 21 + 3) and remove 3 sticks.

23. Fibonacci nim: The next move III. A total of 24 sticks have been removed leaving 66. Since 66 = 55 + 8 + 3, you can keep your winning position by removing only 3 sticks.

2.3. Prime cuts of numbers

Developing Ideas

1. **Primal instincts**. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

2. **Fear factor.** $6 = 2 \cdot 3,\ 24 = 2 \cdot 2 \cdot 2 \cdot 3,\ 27 = 3 \cdot 3 \cdot 3,\ 35 = 5 \cdot 7,\ 120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5.$

3. **Odd couple**. No, n+1 will be an even number greater than 2, and so will have 2 as a factor. If $n = 1$, then n+1 = 2 which is prime.

4. **Tower of power.** The first ten powers of 2 are: 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024. The first five powers of 5 are: 5, 25, 625, 3125, 15,625.

5. **Compose a list.** The list of even numbers starting with 4 contains no primes. The list of powers of 5 starting with 25 contains no primes.

Solidifying Ideas

6. **A silly start.** It's a personal choice, but 51 has our vote. Nothing about the number screams that its factors are 3 and 17. Another favorite is 91 = 7 x 13.

7. **Waiting for a nonprime.** When $n = 4$, the resulting number is 25 which isn't prime. In fact, most of the time the constructed number won't be prime. The next prime number doesn't occur until $n = 11$.

8. **Always, sometimes, never.** By definition, a product of two numbers is not prime, so "Never" is the answer to both questions.

9. **The dividing line.** Sometimes. For example, 8/4 = 2 is prime, but 16/4 = 4 is not.

10. **Prime power.** No. Raising to a power stands for repeated multiplication, and so the resulting number would be represented as a product of numbers, a definite giveaway of its non-prime status.

11. **Nonprimes.** Besides 2, all the even numbers are non-primes. So there are infinitely many numbers that are not prime.

12. **Prime test.** No. The crux of the definition of *prime* is that no other numbers other than 1 and n divide into n. For example, 1 and 4 both divide into 4 evenly, but 4 is not prime. The numbers 1 and n will always divide into n evenly, for any number n.

13. **Twin primes.** (3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73), (101,103), (107,109), (137,139), (149,151), (179,181), (191,193), (197,199)

Do you think it becomes harder and harder to find twin primes as we look at larger and larger prime numbers? ... Or does their distribution appear random?

14. **Goldbach.** 4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 3 + 7, 12 = 5 + 7, 14 = 3 + 11, 16 = 3 + 13, 18 = 5 + 13, 20 = 3 + 17, 22 = 3 + 19, 24 = 5 + 19, 26 = 3 + 23, 28 = 5 + 23, 30 = 7 + 23

Note that as the numbers get larger, there are more ways to express the number as a sum of two primes. 32 = 3 + 29, 11 + 19, 13 + 17, etc..

15. **Odd Goldbach.** The smallest counter-example is 11. The sum of two odd primes is an even number, so if we are to represent 11 as such a sum, 2 will be one of the primes. The other number is then 11 – 2 = 9, but 9 isn't prime.

16. **Still the 1.** The harder question is, "Are any of these prime?" We can describe each element in the list by its number of digits. If it has an even number of digits, then the number is divisible by 11. If it has 3,6,9,... digits, then the number is at least divisible by 111. So the only candidates for prime numbers are those whose length is itself a prime! By computer search, the first three primes in the sequence have 19, 23, and 317 digits.

17. **Zeros and ones.** 1001 = 13 x 11 x 7 is the first non-prime in the sequence.

18. **Zeros, ones, and threes.** This sequence includes several primes, but they are still few and far between. First non-prime is 1003 = 17 x 59. The next three primes on the list are $10^5 + 3$, $10^6 + 3$, and $10^{11} + 3$.

19. **A rough count.** The prime number theorem states that the number of primes less than 10^{10} is about $10^{10} / \ln(10^{10})$ or just over 400 million.

20. **Generating primes.** The first non-prime given by the sequence $n^2 + n + 17$ occurs for $n = 16$. The resulting number is $289 = 17 \times 17$. The first non-prime for $n^2 - n + 41$ occurs for n = 41. What are the factors of the corresponding number?

21. **Generating primes II.** These are the Mersenne primes, and the first non-prime of this form is $2^{4-}1 = 15$.

22. **Floating in factors.** The answer is the product of the three smallest prime numbers, $2 \times 3 \times 5 = 30$.

23. **Lucky 13 factor.** Call the mystery number X. The first statement allows us to express X as $13A + 7$ for some unknown A. The number less one, $X - 1 = 13A + 6$, is still not divisible by 13. If we subtract 7, then we get $X - 7 = 13A$, and this is divisible by 13. So the answer is 7.

24. **Remainder reminder.** As in Mindscape 23, we write the original number as $X = 13A + 7$. Adding 22 yields, $X + 22 = 13A + 7 + 22 = 13A + 29 = 13A + 13 \times 2 + 3 = 13(A + 2) + 3$. So 13 goes into our new number $(A + 2)$ times with a remainder of 3.

25. **Remainder roundup.** As in Mindscapes 23, 24, write $X = 91A + 52$. Then $X + 103 = 91A + 155$. Recognize that $91 = 7 \times 13$, and $155 = 22 \times 7 + 1$, so that we can write $X + 103 = 7(13A) + 7 \times 22 + 1 = 7(13A + 22) + 1$. Final answer is 1.

Creating New Ideas

26. **Related remainders.** The first line allows us to write our two numbers, X and Y, in the following way: $X = 57A + r$, and $Y = 57B + r$. So $(X - Y) = 57A - 57B = 57(A - B)$, and 57 definitely divides this number. Because $57 = 3 \times 19$, 3 and 19 will also divide $(X - Y)$.

    Suppose we divide two numbers by some integer m. The two numbers will have the same remainder upon division if and only if m is a factor of the difference.

2.4. Crazy Clocks and Checking Out Bars

Developing Ideas

1. A flashy timepiece. Twelve hours after 3:00, your watch will again show 3:00. Because $14 = 12 + 2$, in 14 hours your watch will show 5:00, 2 hours after 3:00. Because $25 = 2 \times 12 + 1$, in 25 hours your watch will show 4:00, just 1 hour after 3:00. Because $240 = 20 \times 12$, in 240 hours your watch will show 3:00 again.

2. Living in the past. Twenty-four hours before 8:00 your watch showed 8:00. Because $10 + 2 = 12$, 10 hours earlier it showed 10:00; 25 hours earlier, it showed 7:00; 2400 hours earlier, it showed 8:00.

3. Mod prods. $16 \equiv 2 \pmod 7$; $24 \equiv 3 \pmod 7$; $16 \times 24 = 384 \equiv 6 \pmod 7$; $[16 \pmod 7 \times 24 \pmod 7] = 2 \times 3 = 6$. The last two quantities are equal.

4. Mod power. $7 \equiv 1 \pmod 3$; $7^2 \equiv 1 \pmod 3$; $[7 \pmod 3]^2 = (1)^2$, which equals $7^2 \pmod 3$. $7^{1000} \pmod 3 \equiv [7 \pmod 3]^{1000} \equiv 1^{1000} \equiv 1 \pmod 3$.

5. A tower of mod power. $13 \equiv 2 \pmod{11}$; $13^2 \pmod{11} \equiv 169 \pmod{11} \equiv 4 \pmod{11}$. Note that $[13 \pmod{11}]^2 = 13^2 \pmod{11}$. Also, $13^3 \pmod{11} \equiv [13 \pmod{11}]^3 \equiv 2^3 \pmod{11} \equiv 8 \pmod{11}$. Finally, $13^4 \pmod{11} \equiv [13 \pmod{11}]^4 \equiv 2^4 \pmod{11} \equiv 16 \pmod{11} \equiv 5 \pmod{11}$.

Solidifying Ideas

6. Hours and hours. Because $96 = 8 \times 12$, the clock will complete 8 full revolutions after 96 hours leaving the hand positions unchanged. Because $1063 = 88 \times 12 + 7$, after 1063 hours the clock will spin completely around 12 times, and then spin 7 more hours' worth, leaving the hands at 5:45. Because $-23 = -2 \times 12 + 1$, 23 hours before 7:10 the clock read 8:10. Similarly, 108 hours earlier, the clock read 7:10 because $-108 = -9 \times 12$.

7. Days and days. $3724 = 532 \times 7$ and $365 = 52 \times 7 + 1$. So in 3724 days it will still be Saturday, while the 365^{th} day from now will fall on a Sunday.

8. Months and months. Express each number as a simpler number mod 12. ($219 = 18 \times 12 + 3$; $120{,}963 = 10080 \times 12 + 3$; $-89 = -7 \times 12 - 5$; or $-8 \times 12 + 7$...) 219 months from now will be October (July + 3), and so will 120,963 months from now. Because -89 divided by 12 has a remainder of -5, we need only go back 5 months to February.

9. Celestial seasonings. Compute $3 \times 0 + 1 \times 7 + 3 \times 1 + 1 \times 7 + 3 \times 3 + 1 \times 4 + 3 \times 0 + 1 \times 0 + 3 \times 0 + 1 \times 2 + 3 \times 1 + 1 \times 8 = 43$. Because the sum is not evenly divisible by 10, it is not a correct UPC. The corresponding sum for the next two codes is 40 and 42 respectively. So the second code is the correct one.

10. SpaghettiOs. (See Mindscape 9.) Because the sums are 41, 49, and 50 respectively, the third number is correct.

22. More bank checks. (See Mindscape 21.) With the missing digit represented by D, the sums are $171 + 9D$ and $84 + 9D$ respectively. So the correct codes are 6 2 9 1 0 0 2 7 1 and 5 5 0 3 1 0 1 1 4. In the second example, $84 \equiv 4 \pmod{10}$ so we need $9D \equiv 6 \pmod{10}$ and the only value of D that satisfies this equation is $D = 4$.

23. UPC your friends. Answers will vary.

24. Whoops. In each example, two changes were made, and they canceled each other out. In the first code, the 9th and 11th digits were switched. Because the sum is computed by multiplying the 9th digit by 3 and the 11th digit by 3, the sum doesn't change. Similarly, for the second example, the 3rd and 8th digits are changed. Instead of the sum equaling .... + 3 × 1 + ... + 1 × 2 + ... , we have ... + 3 × 0 + ... + 1 × 5 + ..., where the ... represents parts of the sum that are unchanged. Because 3 × 1 + 1 × 2 = 3 × 0 + 1 × 5, the sum remains unchanged.

25. Whoops again. (See Mindscape 24.) In the first code, the 1st and 4th digits are changed, so instead of 7 × 0 + ... + 7 × 7 + ... we have 7 × 7 + ... + 7 × 0 + ..., and so the sum remains unchanged. The same type of mistake occurs in the second example where the 6th and 9th terms are interchanged. Because the 6th and 9th terms are both multiplied by the same weight, 9, the total sum will remain unchanged.

Creating New Ideas

26. Mod remainders. $129 = 9 \times 13 + 12$, so 12 is the remainder when 129 is divided by 13. We can also say $129 \equiv 12 \pmod{13}$. A quick way to see this is $129 = 130 - 1 = 10 \times 13 - 1 = 9 \times 13 + 13 - 1 = 9 \times 13 + 12$. You would spin around 13 times and then move the clock ahead 12 hours more.

27. More mod remainders. $2015 = 287 \times 7 + 6$. So $2015 \equiv 6 \pmod{7}$. If m divided by n gives a remainder r, then we can say $m \equiv r \pmod{n}$. If we had a clock with n hour positions (0 through $n - 1$), then after moving the hour hand of the clock m places, the hand will be sitting in the r^{th} positions.

28. Money orders. Because 6830910275 is divisible by 7, the check digit is 0.

29. Airline tickets. We have $10061559129884 = 1437365589983 \times 7 + 3$, so the check digit is 3.

30. UPS. (See Mindscapes 28–29.) $84200912 = 12028701 \times 7 + 5$, so the check digit is 5.

31. Check a code. Check the identification number on your example using the technique in Mindscape 28 or 29.

32. ISBN. Verify this check method for the ISBN of this book.

2.5. Secret Codes and How to Become a Spy

Developing Ideas

1. **What did you say?** THIS IS THE CORRECT MESSAGE.

2. Secret admirer. The message encodes to: B WXAU GXL.

3. **Setting up secrets.** The numbers $p = 7$ and $q = 17$ are both prime because each has no factor other than itself and 1. The number $m = (p\text{-}1)(q\text{-}1) = 6 \times 16 = 96$. The number e = 5 has no factors in common with m = 96. Finally, $5 \times 77 - 96 \times 4 = 385 - 384 = 1$

4. Second secret setup. The numbers $p = 5$ and $q = 19$ are both prime because each has no factor other than itself and 1. The number $m = (p\text{-}1)(q\text{-}1) = 4 \times 18 = 72$. The number $e = 11$ has no factors in common with $m = 72$. Finally, $11 \times 59 - 72 \times 9 = 649 - 648 = 1$.

5. **Secret squares.** We find $2^2 = 4 \underline{=} 1 \pmod 3$; $3^2 = 9 \underline{=} 0 \pmod 3$; $4^2 = 8 \underline{=} 2 \pmod 3$; $5^2 = 25 \underline{=} 1 \pmod 3$. As you successive integers, the result (mod 3) cycles through the pattern 1, 0, 2, 1, 0, 2, ….

Solidifying Ideas

6. Petit Fermat 5. The expressions are all of the form $n^{(p-1)} \pmod p$, and so by Fermat's Little Theorem, they are equal to 1 (mod p). e.g. $4^4 = (4^2)^2 = (16)^2 = 1^2 = 1 \pmod 5$, where the second to last equality results because $16 \equiv 1 \pmod 5$.

7. Petit Fermat 7. As in question 1, the numbers are all of the form $k^{(p-1)} \pmod p$, and so are equal to 1 (mod 7).

8. Top secret. The encoded word is $4^7 \pmod{143} \equiv 82$. To decode the number, raise the encrypted information to the 103rd power and compute the remainder (mod 143).

9. Middle secret. You don't need to compute 3^7 explicitly. $3^5 \equiv 243 \equiv 100 \pmod{143}$, so $3^6 \equiv 3 \times 100 \equiv 14 \pmod{143}$ and finally $3^7 \equiv 3 \times 14 \equiv 42 \pmod{143}$. As in Mindscape 8, the information is decoded by the computation $42^{103} \equiv 3 \pmod{143}$.

10. Bottom secret. We need to compute $11^7 \pmod{143}$. ($11^7 = 19{,}487{,}171$). Because $19{,}487{,}171 \div 143 = 136{,}273$ with a remainder of 132, we have $11^7 \pmod{143} \equiv 132$. The original '101 can be recovered by computing $132^{103} \equiv 11 \pmod{143}$. Even though the encoded number is identical to the original number, it's still a secret because you are the only person who knows that they are one and the same.

11. Creating your code. Note first $m = (3 - 1) \times (5 - 1) = 8$. Because e must be relatively prime to m, we need only consider the values $e = 1$, 3, 5, and 7. For each possible value of e, find d and y that satisfy $de - 8y = 1$. For example, for $e = 1$, fill in the following blanks: __ x 1 − 8 x __ = 1. Because $1 \times 1 - 8 \times 0 = 1$, ($e = 1, d = 1$) is a pair. Similarly, because $3 \times 3 - 8 \times 1 = 1$, $5 \times 5 - 8 \times 2 = 1$, and $7 \times 7 - 8 \times 6 = 1$, ($e = 3$, $d = 3$), ($e = 5$, $d = 5$), and ($e = 7$, $d = 7$) are all pairs.

12. Using your code. "HI" becomes (08) (09). To use the coding scheme ($p = 3$, $q = 5$, e = 3, $d = 3$), we need to compute $8^3 \equiv 2 \pmod{15}$ and $9^3 \equiv 9 \pmod{15}$. So the code is (02)(09) or "BI". Because $2^3 \equiv 8 \pmod{15}$ and $9^3 \equiv 9 \pmod{15}$ we get the original message back upon decoding. Note that you can only use the first 14 letters of the alphabet!

13. Public secrecy. Using $83^7 \equiv 8 \pmod{143}$, the encoded version is '8'. One deciphers this message with the formula $8^{103} \equiv 83 \pmod{143}$.

14. Going public. You encode '61' by computing $61^7 \equiv 74 \pmod{143}$, and you decode '74' by computing $74^{103} \equiv 61 \pmod{143}$.

15. Secret says. Use $38^{103} \equiv 103 \pmod{143}$ to obtain the original message, '103'.

Creating New Ideas

16. Big Fermat. The hint asks you to recall that $5^6 \equiv 1 \pmod{7}$. This means that $(5^6)^k \equiv 1^k \equiv 1 \pmod{7}$ for any integer k. In particular, because $600 = 6 \times 100$, it is convenient to choose $k = 100$, giving us $5^{600} \equiv (5^{6 \times 100}) \equiv (5^6)^{100} \equiv 1^{100} \equiv 1 \pmod{7}$. Similarly, because $1000000 = 10 \times 100000$, $8^{1000000} \equiv 1 \pmod{11}$.

17. Big and powerful Fermat. (See also solution to Mindscape 16.) Our building block is the formula $5^6 \equiv 1 \pmod{7}$. Now after dividing 668 by 6 we can represent $668 = 6 \times 111 + 2$. Therefore,

$$5^{668} \equiv 5^{6 \times 111 + 2} \equiv 5^{6 \times 111} \times 5^2 \equiv (5^6)^{111} \times (25) \equiv 1^{111} \times 4 \equiv 4 \pmod{7}.$$

18. The value of information. You would have to answer the following questions: Who am I keeping this from? How much time would they be willing to spend trying to break the code? With their resources, what size numbers can they factor in that time? As a reference point, you might note that Maple, a standard mathematical computer package, can factor the product of two 29 digit primes in 30 seconds on a Linux workstation! For every 3 digits you tack on, Maple takes *twice* as long to complete the factorization. With two 32-digit primes, it takes 1 minute; 35-digit primes, 2 minutes; 50-digit primes, 1 hour! (How large would the primes need to be in order for Maple to require 100 years' worth of computation time?)

2.6 The Irrational Side of Numbers

Developing Ideas

1. **A rational being.** A rational number is a number that can be expressed as a fraction - the ratio (or quotient) of two whole numbers.

2. **Fattened fractions.** 6/24 = 1/4, 15/9 = 5/3, -14/42 = -1/3, 125/10 = 25/2, -121/11 = -11.

3. **Rational arithmetic**. $\frac{1}{2}+\frac{5}{2}=\frac{6}{2}=3$; $\frac{1}{2}-\frac{2}{3}=\frac{3}{6}-\frac{4}{6}=-\frac{1}{6}$; $\frac{1}{2}\times\frac{6}{5}=\frac{6}{10}=\frac{3}{5}$;
$\frac{1/2}{2/3}=\frac{1}{2}\times\frac{3}{2}=\frac{3}{4}$; $\frac{5/2\times 6/5}{2/3}=\frac{30/10}{2/3}=\frac{3}{1}\times\frac{3}{2}=\frac{9}{2}$

4. **Decoding decimals.** 0.02 = 2/100, 6.23 = 623/100, 2.71828 = 271,828/100,000, -168.5 = -1685/10, -0.00005 = -5/10,0000.

5. **Odds and ends**. The squares are 1, 4, 9, 16, 25, 36, 49, 64, 81, 100. The even numbers have even squares and the odd numbers have odd squares.

Solidifying Ideas

6. Irrational rationalization. No, 3√2/5√2 = 3/5, which is rational. The product or quotient of an irrational and a rational is always irrational, so both 3√2 and 5√2 are irrational. But the quotient (or product) of two irrationals is not always irrational.

7. Rational rationalization. Yes, the quotient of two rationals is rational. If a,b,c, and d are integers, then (a/b) / (c/d) = (ad)/(bc) which is rational by definition; it is the quotient of two integers.

8. Rational or not. √2/14 is the only irrational number in the list. As the ratio of two integers, 4/9 is rational by definition. 1.75 = 1 + 3/4 = 7/4, √20/(3√5) = (√20/√5)/3 = √4/3 = 2/3, 3.14159 = 314159/100000. We could reason that 3.14159 and 1.75 are rational because they each have a repeating decimal expansion (1.7500000..., 3.13159000...)

9. Irrational or not. All but $\sqrt{3}/3$ are rational. $\sqrt{16}/20 = 4/5$, $12/7.5 = 120/75$, $-147 = -147/1$, $0 = 0/1$. $\sqrt{3}/3$ is the quotient of an irrational and a rational number and therefore irrational.

10. $\sqrt{5}$. The proof is identical to the proof of the irrationality of $\sqrt{2}$, except that the notions *even* and *odd* are replaced with *divisible by 5* and *not divisible by 5*, respectively. Assume $\sqrt{5} = b/c$ with b and c having no common factors. We have $b^2 = 5c^2$, implying b is divisible by 5 (because 5 is prime and must therefore appear as one of the prime factors of b; we're using the uniqueness of the prime factorization here). Expressing $b = 5d$ gives, $25d^2 = 5c^2$ or $5d^2 = c^2$ implying c is *also* divisible by 5, a contradiction. This same idea can be applied to the square root of any prime number.

11. $2\sqrt{3}$. Though you can mimic the proof that $\sqrt{2}$ is irrational, it is simpler to note that because 3 is prime, if follow that $\sqrt{3}$ is irrational (see Mindscape 10), and then argue that a rational multiplied by an irrational is irrational.

12. $\sqrt{7}$. Identical in spirit to Mindscape 10.

13. $\sqrt{3} + \sqrt{5}$. An alternate style of proof: $(\sqrt{3} + \sqrt{5})^2 = (\sqrt{3} + \sqrt{5})(\sqrt{3} + \sqrt{5}) = 3 + 2\sqrt{3}\sqrt{5} + 5 = 8 + 2\sqrt{15}$. First argue that $\sqrt{15}$ is irrational (see Mindscape 15). Use the fact that a rational times an irrational is irrational to show that $2\sqrt{15}$ is irrational. Similarly, the sum of a rational and an irrational is also irrational, which implies that $8 + 2\sqrt{15} = (\sqrt{3} + \sqrt{5})^2$ is irrational. If $(\sqrt{3} + \sqrt{5})$ were rational, then $(\sqrt{3} + \sqrt{5})^2$ would be rational too. Because $(\sqrt{3} + \sqrt{5})^2$ is *not* rational, $(\sqrt{3} + \sqrt{5})$ is not rational either, completing the proof.

14. $\sqrt{2} + \sqrt{7}$. Model the text's proof that $\sqrt{2} + \sqrt{3}$ is irrational. Assume $\sqrt{2} + \sqrt{7} = a/b$ (in lowest terms). $(\sqrt{2} + \sqrt{7})^2 = 9 + \sqrt{14} = a^2/b^2$, so that $\sqrt{14} = a^2/b^2 - 9 = (a^2 - 9b^2)/b^2$ contradicting the fact that $\sqrt{14}$ is irrational (see Mindscape 15).

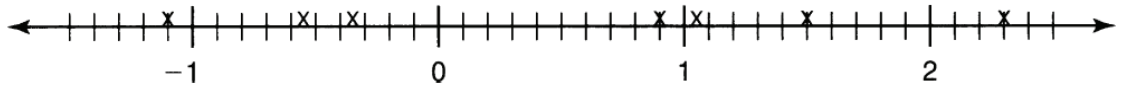
15. $\sqrt{10}$. We need a slight modification of the proof in Mindscape 10. Begin the same way: Assume $\sqrt{10} = c/d$ with *c* and *d* having no common factors. Squaring gives $c^2 = 10d^2$. Because the right hand side is divisible by 5, the left hand side is divisible by 5 as well. This means that *c* is divisible by 5. (If *c* weren't divisible by 5, then c^2 wouldn't be divisible by 5 either.) Write $c = 5n$, substituting gives $25n^2 = 10d^2$, or $5n^2 = 2d^2$. Now we must work harder to show that 5 divides *d*. Imagine writing out the prime factorization for the left and right sides of the equation. On the left we have all the prime factors of *n* (listed twice) and 5. On the right we have 2 and all the prime factors of *d* (listed twice). Because both sides represent the same number, we call upon the uniqueness of prime factorizations to argue that the list of primes on both sides are the same. Because the prime 5 appears on the left side, it must also appear on the right side. And because it can only come from the prime factorization of *d*, we must have that 5 is a prime factor of *d*. So d is divisible by *5* and we have our contradiction.

16. $1 + \sqrt{10}$. If $1 + \sqrt{10} = a/b$, then $\sqrt{10} = a/b - 1 = (a - b)/b$ is rational. Mindscape 15 shows that this is not the case. This contradiction shows that our assumption was wrong, proving that $1 + \sqrt{10}$ is irrational.

2.7. Get Real

Developing Ideas

1. X marks the "X-act" spot. The X's on the number line below mark the approximate locations, from left to right, of the numbers –1.1, -0.55, -1/3, 0.9, 1.05, 3/2, and 2.3,



2. **Moving the point**. Simplifying we get 10 × (3.14)=31.4, 1000x(0.123123…)=123.123123…, 10 × (0.4999…)=4.999…, $\frac{98.6}{100} = 0.986$, $\frac{0.333...}{10} = 0.0333...$

3. **Watch out for ones!** Using long division we find 1/9 = 0.111….

4. **Real redundancy.** If M = 0.4999…, then 10M = 4.999…. We find 10M – M = 9M and it also equals 4.999… - 0.4999… = 4.5. Then 9M = 4.5, so M = 4.5/9 = 0.5. Thus 0.4999… = 0.5.

5. Being irrational. A number is irrational if it is not rational, i.e., it *cannot* be written as a ratio of two integers.

Solidifying Ideas

6. Always, sometimes, never. Sometimes. By 'an unending decimal expansion' we mean a number whose decimal doesn't end in a trail of zeros All numbers ending in a trail of zeros are rational, but the converse is not true. for example, 9/7 = 1.285714285714285714285714285714... is rational, but 1.010010001000010000010000001... is irrational.

7. Square root of 5. False: if the decimal expansion for √5 eventually repeated, we could use the ideas in the text to express √5 as the ratio of two integers and so prove that √5 is rational. Because we proved √5 irrational in the Section 2.6, this can't happen; so the only alternative is that the decimal expansion for √5 does not repeat.

18. 20.4545 . Note that this decimal stops or ends in a trail of zeros (20.454500000…). Thus the method of Mindscape 17 will work here, too. 20.4545 = 204545/10000. It isn't necessary to reduce the fraction to lowest terms, but if you were curious, $X = 40909/2000$.

19. 12.999 . Because the decimal ends, we can eliminate the decimal by multiplying it by 1000. So write 12.999 = 12.999/1 = (12.999/1) × (1000/1000) = 12999/1000.

20. 2.22... . X = 2.22222…. Because the number has a segment of length one that repeats, multiply the number by 10 to shift the decimal point by exactly one digit. $10X = 22.22222…$ Now subtract, $10X – X =$ 22.22222… – 2.22222… = 20 (Note that all digits to the right cancel exactly.) So $9X = 20$, and $X = 20/9$.

21. 43.12... . Call our elusive number X, so that $X = 43.121212…$ Because there are two digits in our repeating segment, multiply X by 100 to shift the decimal points by two digits. $100X = 4312.121212…$ Subtracting gives $100X – X = 4312.121212… – 43.121212 = 4269$. Together we get 99X = 4269 or $X =$ 4269/99 = 1423/33. (Again simplifying fractions is not necessary!)

22. 5.6312... . Follow the reasoning in Mindscape 21. $X = 5.63121212…$, $100X = 563.12121212…$ $100X – X = 563.121212… – 5.6312121212… = 557.49$ We still have a decimal number, but at least it stops! Solving for X in $99X = 557.49$ gives $X = 557.49/99$. Now multiply both numerator and denominator of the fraction by 100 to eliminate the decimal points. $X = 55749/9900 = 18583/3300$.

23. 0.01... . $X = 0.010101…$ Because the repeating segment has length 2, multiply by 100 to shift the decimal point two digits to the left. $100X = 1.010101…$ Subtracting gives $100X – X = 1.010101 –$ 0.010101 = 1 so that $99X = 1$, or $X = 1/99$.

24. 71.2399... . Note that this number can also be represented as 71.24 which is equal to 7124/1000. However, we could still use the ideas from Mindscape 22 to get this fraction. $X = 71.239999…$ $10X =$ 712.39999…, $10X – X = 712.39999… – 71.239999… = 641.16$ so that $9X = 641.16$, or $X = 641.16/9 =$ 64116/900 = 7124/1000 = 1781/25.

25. Just not rational. This number has a pattern (one 0, one 1, two 0s, one 1, three 0s, one 1, etc.), but that does not mean that it's rational. A decimal is rational if and only if there exists a fixed string of digits that repeats forever. This number has no repeating sequence. Suppose there was a repeating sequence of length N. If the repeating sequence were all zeros, then we'd end up with a rational number. If the repeating sequence were not all zeros, then eventually we would see a non-zero digit after every N digits. But this isn't the case; we see arbitrarily large sequences of zeros. This implies that there is no repeating sequence and so the number is irrational.

31. Irrational with 1's and 2's. In Mindscape 25, we showed that $x = 0.01001000100001\ldots$ was irrational. By the same reasoning, $y = 0.21221222122221\ldots$ is also irrational. You could also argue that because $y = 2/9 - x$, the irrationality of x implies the irrationality of y because the sum of an irrational and a rational is always irrational. And finally, for fun, a more interesting, more random looking irrational number with only 1's and 2's: List all the rational numbers, and apply Cantor's diagonalization argument with a rule like, "If the nth digit is a 1, put a 2, otherwise put a 1."

32. Irrational with 1's and Some 2's. No; if only a finite number of 2's appeared in the decimal expansion, then after the last 2, the decimal tail would be all 1's and therefore repeating. So the number would be rational.

33. Half steps. This is Zeno's paradox. You will land on the numbers 1/2, 1/4, 1/8, $1/2^4$, $1/2^5$, $1/2^6$, … , $1/2^n$, … The nth step takes you to $1/2^n$, so you will never get to zero in a finite amount of time. You can get arbitrarily close, but you will never actually get there because $1/2^n$ doesn't equal zero for any finite number n. The limit of this sequence of numbers is zero, but none of the numbers themselves are zero.

34. Half steps again. Suppose the left half of your segment has length L. L may be small, but it is a positive number, and because the sequence $1/2^n$ tends to zero as n grows without bound, there exists some N such that $1/2^N < L$. This means that after N steps, your segment will contain the origin. Note that your center will never hit the origin, but at least some part of you will get to where you want to go.

35. Cutting π. This is an alternate way of asking whether π might be a rational number. Suppose we divided the interval into N pieces. The endpoints land on $3 + 1/N$, $3 + 2/N$, $3 + 3/N$, etc... all of which are rational numbers. Because π is irrational, there is no way that we can represent π as $3 + I/N$ for any integers I and N.

Further Challenges

36. From infinite to finite. How about our favorite irrational number √2? Because we proved it irrational, we know that the decimal is unending and non-repeating. By definition its square is 2, which has a terminating decimal representation.

37. Rationals. Assume x and y are two different positive numbers and that y is bigger than x. The sequence 1/2, 1/3, 1/4, 1/5, … gets arbitrarily small; thus, for some number N, the value of $1/N$ is smaller than the difference $y - x$. Now imagine cutting up the real number line with hash marks every $1/N$ units apart. So you mark 0, $1/N$, $2/N$, $3/N$, … and so on. All these hash marks are on rational numbers, but at least one of the hash marks lies between the numbers x and y because $y - x$ is greater than $1/N$.

38. Irrationals. The argument used in Mindscape 37 could be used here as well. Instead of using hash marks at $1/N$, $2/N$, $3/N$, … use hash marks at $1/N - \sqrt{2}$, $2/N - \sqrt{2}$, $3/N - \sqrt{2}$, etc. But there is a simpler argument: Assume that x and y are positive real numbers with x smaller than y, and let N be such that $1/N$ is smaller than $y - x$. If x is irrational, then $x + 1/N$ is also irrational and lies between x and y; done. If x is