Solutions to Problems for Mathematics 2.5 DV
Date: April 14, 2010[1]

Solution to Problem 1. The equation is $75 = 12 \times 6 + 3$.

Solution to Problem 2. The remainder is 1. This is because 11 evenly divides the first term (i.e., the long product), since 11 is one of its factors, and then 1 is added.

Solution to Problem 3. In fact, the number in question, call it N, cannot have any divisor other than 1 that is less than or equal to n. This is because if $k > 1$ is a number less than or equal to n, then k divides evenly the first term (i.e., the long product), since it is one of its factors, and then 1 is added.

Solution to Problem 4. No, because the number will have a divisor different from 1 and itself (namely, the large integer you raised to a very large power will be a divisor).

Solution to Problem 5. Assume, on the contrary, that m is not a prime number. Then m has a divisor d such that $1 < d < m$. As m is a divisor of n, the integer d is also a divisor of m. This, however contradicts the assumption that m is the smallest divisor of n different from 1 (namely, $1 < d < m$). This contradiction shows that the assumption that m is not a prime number was wrong. Thus, m is indeed a prime number, as claimed.

Solution to Problem 6. Yes. For example, no even positive integer other than 2 is a prime.

Solution to Problem 7. The first one is divisible by two, since the first term (i.e., the long product) is divisible by 2 (since it is one of its factors), and then you add 2. Similarly, the second number is divisible by 3, the third one by 4, the fourth one by 5, the fifth one by 6, and the sixth one by 7.

Solution to Problem 8. The method we will use is called the Sieve of Eratosthenes. We start out by writing down all the integers from 1 to 200:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200.
(when following this along, it is best to write these numbers in a nice table, ten in a row). Then cross out 1 (since it is not a prime number) and then cross out all the numbers that are multiples of 2, except that do not cross out 2 itself. 2 itself is of course a prime number. Then the numbers that have not been crossed out are as follows:
2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199.
(when following along, do not write a new table; just cross out the numbers in the original table). The first surviving number (other than 2) is 3. Since it has not been crossed out, it is a prime number. Now, cross out all the multiples of 3 other than 3 itself (it is best to cross out these numbers in a different way – perhaps by

[1]Notes by Attila Máté, Department of Mathematics, Brooklyn College of CUNY, April 14, 2010. All computer processing for this document was done under Red Hat Linux. $\mathcal{AMS}$-TEX was used for typesetting. PICTEX was used for the diagrams.The programming language Perl was used for separating the problems from the solutions, and for generating the data points for some of the diagrams.

a line going in a different direction, or, better yet, by a pencil of a different color, so that later one can tell which numbers were crossed out on account of being a multiple of 2, and which were crossed out on account of being multiples of 3). It is simplest to cross out even those numbers that have already been crossed out earlier; the multiples of three are easy to find, since if you wrote the numbers with ten numbers in a row, the multiples of 3 are situated along diagonals running from top right to bottom left. The surviving numbers are as follows:
2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97, 101, 103, 107, 109, 113, 115, 119, 121, 125, 127, 131, 133, 137, 139, 143, 145, 149, 151, 155, 157, 161, 163, 167, 169, 173, 175, 179, 181, 185, 187, 191, 193, 197, 199.
The first number not crossed out is 5 (other than the numbers 2 and 3, whose multiples have already been crossed out). Next cross out all the multiples of 5, except 5 itself. The remaining numbers are:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 91, 97, 101, 103, 107, 109, 113, 119, 121, 127, 131, 133, 137, 139, 143, 149, 151, 157, 161, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199.
The first new number (i.e., other than the numbers 2, 3, and 5) is 7. Hence 7 is a prime number. It is worth to reflect a moment why this is: if 7 were not a prime number, it would be crossed out as a multiple of one of its prime divisors. (Recall that the smallest positive divisor other than 1 of a number is a prime. If 7 were not a prime, its smallest positive divisor other than 1 would be a prime less than 7; however, all the multiples of primes less than 7 have already been crossed out; thus, were 7 not a prime, it would have been crossed out).

When crossing out the multiples of 7, it worth paying attention to the following fact, in order to save time. A multiple of 7 (other than 7 itself) has the form $7k$, where $k > 1$ is an integer. Now, if k is an integer less than 7 (i.e., if $k = 2, 3, 4, 5, 6$) then the multiples of k have already been crossed out (directly, we only crossed out the multiples of 2, 3, and 5; but the multiples of 4 were also crossed out, since they are multiples also of 2; the multiples of 6 too were crossed out, since they are multiples of 2 and also of 3). Hence, when crossing out the multiples of 7, we have to start with $7k$ for $k = 7$, i.e., with 7^2. The remaining numbers are:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 121, 127, 131, 137, 139, 143, 149, 151, 157, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199.
When crossing out the multiples of a number, it has been true earlier as well that one has to start with the square of the number. But this would not amounted to a real saving before (the square of 2 is 4, and we started with 4 when crossing out the multiples of 2, the square of 3 is 9, and starting with 9 would have allowed us not to cross out 6 a second time; the square of 5 is 25, but the multiples of 5 are so easy to find that it really did not matter whether we start at 10 or 25).

The first new number that has not been crossed out is 11; hence 11 is a prime. When crossing out the multiples of 11, we have to start with its square, i.e., with 121. After crossing out the multiples of 11, the remaining numbers are
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 169, 173, 179, 181, 191, 193, 197, 199.
The first new number that has not yet been crossed out is 13. Hence 13 is a prime; we next cross out the multiples of 13 starting with $13^2 = 169$. The following numbers are left:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199.
The first new number that has not been crossed out is 17; hence 17 is a prime. We next will have to cross out the multiples of 17, starting with $17^2 = 289$. However 289 is is off this table, so we no longer have to cross out anything. All the remaining numbers in the table are primes.

Solution to Problem 9. We have $7 + 52 = 59 = 4 \times 12 + 11$, that is $7 + 52 \equiv 11 \mod 12$. Therefore it will be 11 o'clock.

Solution to Problem 10. $3 \times 0 + 4 + 3 \times 1 + 1 + 3 \times 9 + 6 + 3 \times 0 + 1 + 3 \times 0 + 1 + 3 \times 2 + 1 = 50$ and $50 \equiv 0 \mod 10$, so the number is a correct Universal Product Number.

Solution to Problem 11. A positive integer is called a prime if it is greater than 1 and it has no divisor other than one and itself.

Solution to Problem 12. A pair of twin primes are two primes the difference between which is 2. Some pairs of twin primes are $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, and $(41,43)$.

First Solution to Problem 13. By Fermat's Little Theorem, we have $9^{10} \equiv 1 \mod 11$, so $9^{70} \equiv (9^{10})^7 \equiv 1^7 \equiv 1 \mod 11$, so $9^{74} \equiv 9^{10} \cdot 9^4 \equiv 1 \cdot 9^4 \equiv 9^4 \mod 11$. Now, $9^2 \equiv 81 \equiv 4 \mod 11$, so $9^4 \equiv (9^2)^2 \equiv 4^2 \equiv 16 \equiv 5 \mod 11$. Thus $9^{74} \equiv 9^4 \equiv 5 \mod 11$.

Second Solution to Problem 13. One can directly calculate 9^{74}, without using Fermat's Little Theorem. This is somewhat more work. The best way to do this is to use repeated squaring whenever possible. Note that $74 = 2 \times 37 = 2 \times (2 \times 18 + 1)$, and $18 = 2 \times 9 = 2 \times (2 \times 4 + 1)$. So one can calculate 9^{74} by following these equations backwards, as follows.

$9^2 \equiv 81 \equiv 4 \mod 11$, so $9^4 \equiv (9^2)^2 \equiv 4^2 \equiv 16 \equiv 5 \mod 11$. Then $9^8 \equiv (9^4)^2 \equiv 5^2 \equiv 25 \equiv 3 \mod 11$. Next, $9^9 \equiv 9^8 \times 9 \equiv 3 \times 9 \equiv 27 \equiv 5 \mod 11$. Hence $9^{18} \equiv (9^9)^2 \equiv 5^2 \equiv 25 \equiv 3 \mod 11$. Therefore, $9^{36} \equiv (9^{18})^2 \equiv 3^2 \equiv 9 \mod 11$. So $9^{37} \equiv 9^{36} \times 9 \equiv 9 \times 9 \equiv 81 \equiv 4 \mod 11$. Thus $9^{74} \equiv (9^{37})^2 \equiv 4^2 \equiv 16 \equiv 5 \mod 11$.

Solution to Problem 14. The congruence

$$ac \equiv bc \mod p$$

means that

$$p \mid bc - ac = (b-a)c.$$

A prime number is a divisor of a product only if it is a divisor of (at least) one of the factors. That is, for this to be true, we must have either $p \mid b - a$ or $p \mid c$ (recall that we assumed that p is a prime). The latter does not hold by our assumptions; so we must have $p \mid b - a$. That is,

$$a \equiv b \mod p.$$

This is what we wanted to show.

Notice that without the assumption that p is a prime, the conclusion might not be true. For example, we have

$$10 \cdot 2 \equiv 19 \cdot 2 \mod 6$$

and yet

$$10 \equiv 19 \mod 6$$

Solution to Problem 15. Assuming that two right-hand sides are congruent, subtract the corresponding left-hand sides and factor out 8. The product cannot be divisible by 11, since 11 is a prime, and so it will divide a product only if it divides one of the factors.

For example: Assume we have

$$8 \times 2 \equiv 8 \times 9 \mod 11.$$

Using the Cancelation Law for Congruences (note that 11 is a prime and $11 \nmid 8$), we can cancel the multiplier 8 on both sides and conclude that

$$2 \equiv 9 \mod 11.$$

This is, however, not true, and so the congruence

$$8 \times 2 \equiv 8 \times 9 \mod 11$$

cannot be true, either.

If one wants to avoid reference to the Cancelation Law, one can argue directly as follows (note, however, that the argument below repeats the proof of the Cancelation Law):

Assume we have

$$8 \times 2 \equiv 8 \times 9 \mod 11.$$

Then, subtracting the two sides, we have

$$8 \times 9 - 8 \times 2 \equiv 0 \mod 11,$$

that is,

$$8 \times (9-2) \equiv 0 \mod 11,$$

i.e.,

$$8 \times 7 \equiv 0 \mod 11.$$

This means that 8×7 is divisible by 11; in symbols, $11 \mid 8 \times 7$. This is not possible, since neither $11 \mid 8$ nor $11 \mid 7$. (Note: of course, one can easily calculate 8×7, and then note that, clearly, 11 is not a divisor of the result, 56; however, what matters is the principle, and only by paying attention to the principle can one realize that 11 will not be a divisor *in any similar situation.*)[2]

Solution to Problem 16. Consider the congruences $8 \times 1 \equiv n_1 \mod 11$, $8 \times 2 \equiv n_2 \mod 11$, $8 \times 3 \equiv n_3 \mod 11$, $\ldots$, $8 \times 9 \equiv n_9 \mod 11$, $8 \times 10 \equiv n_{10} \mod 11$. The observation just made shows that the numbers n_1, n_2, n_3, $\ldots$, n_9, n_{10}, are ten different numbers between 1 and 10; that is, they are the numbers 1, 2, 3, $\ldots$, 11, 10, in some order. So, if we multiply the congruences together, we have

$$(8 \times 1) \times (8 \times 2) \times (8 \times 3) \times \ldots \times (8 \times 9) \times (8 \times 10) \equiv 1 \times 2 \times 3 \times \ldots \times 9 \times 10 \mod 11.$$

That is,

$$8^{10} \times (1 \times 2 \times 3 \times \ldots \times 9 \times 10) \equiv (1 \times 2 \times 3 \times \ldots \times 9 \times 10) \mod 11.$$

We can cancel the long product on both sides of this congruence to obtain $8^{10} \equiv 1 \mod 11$. This is because

$$(1 \times 2 \times 3 \times \ldots \times 9 \times 10)$$

is not divisible by 11 (since 11 is a prime, and 11 is not a divisor of any of the factors of this product). So, writing the above Congurence as

$$8^{10} \times (1 \times 2 \times 3 \times \ldots \times 9 \times 10) \equiv (1 \times 2 \times 3 \times \ldots \times 9 \times 10) \times 1 \mod 11.$$

(the only change we made was that we multiplied the right-hand side by 1, which means no change at all), and using the Cancelation Law for Congruences we obtain $8^{10} \equiv 1 \mod 11$, which is what we wanted to show.

If we want to avoid the use of the Cancelation Law for Congruences, we can argue as follows (this argument essentially repeats the proof of the Cancelation Law for Congruences):

Subtracting the right-hand side from the left-hand side in the above congruence, we obtain

$$(8^{10} - 1) \times (1 \times 2 \times 3 \times \ldots \times 9 \times 10) \equiv 0 \mod 11,$$

that is

$$11 \mid (8^{10} - 1) \times (1 \times 2 \times 3 \times \ldots \times 9 \times 10)$$

(i.e., 11 is a divisor of the number on the right). However, 11 is a prime number; so, it can be a divisor of a product only if it is a divisor of one of the factors. Clearly, 11 is not a divisor of any of the numbers 1, 2, 3, $\ldots$, 9, 10; hence it must be a divisor of the first factor, $8^{10} - 1$. That is, $8^{10} - 1 \equiv 0 \mod 11$, i.e., $8^{10} \equiv 1 \mod 11$, as we wanted to show.

Solution to Problem 16. If p is a prime number and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$.

Solution to Problem 17. It needs to be noted that that, in codes used in practice much larger numbers must be used. In the example, $143 = 11 \times 13$, and for any integer W not divisible by 143 we have

$$(W^7)^{103} \equiv W^{7 \times 103} \equiv W^{721} \equiv W^{6 \times 10 \times 12 + 1} \equiv W \mod 143;$$

[2]Here 8 was so chosen that $11 \nmid 8$ (in fact, 8 plays the role of a in the statement $a^{p-1} \equiv 1 \mod p$ of Fermat's Little Theorem, and it is explicitly assumed that $p \nmid a$. As for the general reason for the relation $11 \nmid 7$, the number $9 = 9 - 2$ comes about as the difference of two distinct positive integers less than 11, so it must a nonzero number between -11 and 11; so it cannot be divisible by 11.

the last congruence is based on Fermat's Little Theorem; more details are given in the textbook.

Answers to Questions (i)–(vi). (i) Everybody is allowed to know the public key. (ii) Only Bob is supposed to know his secret key. (iii) Alice sends the number $C \equiv W^7 \mod 143$. (iv) Having received the encoded message C, Bob calculates $C^{103} \mod 143$; this is the original message, since $C^{103} \equiv (W^7)^{103} \equiv W \mod 143$ (see above). (v) Bob signs the message W by sending $C \equiv W^{103} \mod 143$ (using his secret key) to Alice. (vi) Alice cannot read the message C, but by calculating $C^7 \mod 143$ (using Bob's public key), the message becomes readable, since $C^7 \equiv (W^{103})^7 \equiv W \mod 143$ (see above), i.e. $C^7 \mod 143$ is the actual clear-text message. (vii) The fact that Alice can read the message C by applying Bob's public key $(7, 143)$, she can safely conclude that the message C could only have been written by using Bob's secret key (i.e., (103,143); however, Alice neither does, nor need to know this secret key to make this conclusion). Since only Bob knows his secret key, the message must have been written by Bob.

Solution to Problem 18. If m is even then $m = 2k$ for some integer k. Then $m^2 = (2k)^2 = 2^2 \cdot k^2 = 4k^2$. That is m^2 is 4 times an integer; i.e., m^2 is divisible by 4.

Solution to Problem 19. If $m^2 = 2n$, then m^2 is even; so m must also be even (since the square of an odd number is odd), i.e., $m = 2k$ for some integer k. Then $m^2 = (2k)^2 = 2^2 \cdot k^2 = 4k^2$. That is $4k^2 = 2n$, and so $2k^2 = n$. Hence, n is twice an integer (namely, twice k^2); i.e, n is even.

Solution to Problem 20. No. Let c be the largest common factor (greatest common divisor, by another name) of m and n. Then $m = kc$ and $n = lc$, where the numbers k and l have no common factor (other than 1). Now $m^2 = (kc)^2 = k^2 \cdot c^2$ and $n^2 = (lc)^2 = l^2 \cdot c^2$. So the equation $m^2 = 2n^2$ becomes $k^2 \cdot c^2 = 2l^2 \cdot c^2$. One can cancel c^2 on both sides to obtain $k^2 = 2l^2$. The right-hand side here is even; so is then the left-hand side. Thus k must be even; i.e., $k = 2u$ for some integer u. Then $k^2 = (2u)^2 = 2^2 \cdot u^2 = 4u^2$.

Thus, the equation $k^2 = 2l^2$ becomes $4u^2 = 2l^2$, i.e., $2u^2 = l^2$. So l must be even. Thus we concluded that k and l are both even. This is a contradiction, since k and l have no common factor. This contradiction means that the starting equation, namely $m^2 = 2n^2$ cannot be true when m and n are nonzero integers.

Of course, the equation is satisfied when $m = n = 0$. Explain why the above argument does not work when $m = n = 0$; this needs to be explained, since the above argument could not be correct if it gave the incorrect conclusion that $m^2 = 2n^2$ cannot hold even if $m = n = 0$.[3]

Note. If this argument is pursued to its natural conclusion, it shows that $\sqrt{2}$ is irrational.

Solution to Problem 21. Assume, on the contrary, that $\sqrt{2}$ is rational. Then there are integers m and n such that $\sqrt{2} = m/n$. We may assume here that the fraction m/n is irreducible. After squaring the above equation, we obtain that $2 = (m/n)^2$, i.e., that $2 = m^2/n^2$. Multiplying both sides by n^2, we obtain that

$$2n^2 = m^2.$$

The left-hand side here is even, so the right-hand side must also be even, i.e., m^2 is even. This means that m must be even, since the square of an odd number is always odd. Thus, we have $m = 2k$ for some integer k. Then $m^2 = (2k)^2 = 4k^2$, and so the above equation can be written as

$$2n^2 = 4k^2;$$

after dividing both sides by 2, we obtain that

$$n^2 = 2k^2.$$

[3]If $m = n = 0$, then the greatest common divisor of m and n is not defined. In practical terms, this means that in this case no numbers c, k, and l can be found with $m = kc$ and $n = lc$ such that c is nonzero and the numbers k and l have no common factors. One could take $c = 0$, but then one could not conclude $k^2 = 2l^2$ from the equation $k^2c^2 = 2l^2c^2$, as we did in the above argument. To see why not, consider why the cancelation of c^2 is in this equation is possible. This equation can be written as $(k^2 - 2l^2)c^2 = 0$. The product on the left-hand side can only be zero if at least one of the factors is zero. Thus, *if* $c^2 \neq 0$, *then* one can conclude that $k^2 - 2l^2 = 0$; but, *if* $c^2 = 0$, *then this conclusion cannot be made.*

The right-hand side here is even, and so the left side must also be even; i.e., n^2 is even. This means that n must be even, since, as we mentioned just before, the square of an odd number is always odd.

We obtained that both m and n even. Thus the fraction m/n can be reduced (by dividing both the numerator and denominator by 2, contradicting our assumption that the fraction m/n is irreducible. This assumption was based on our main assumption that $\sqrt{2}$ is irrational. Since this latter assumption led to a contradiction, this assumption must be false (a correct assumption, combined with correct arguments, cannot lead to a contradiction – if you carefully check the arguments above, you will realize that all the arguments we used were correct). Thus $\sqrt{2}$ must be irrational, as we wanted to show.

Solution to Problem 22. If m is divisible by 3 then $m = 3k$ for some integer k. Then $m^2 = (3k)^2 = 3^2 \cdot k^2 = 9k^2$. That is m^2 is 9 times an integer; i.e., m^2 is divisible by 9.

Solution to Problem 23. If $m^2 = 3n$, then m^2 is divisible by 3; so m must also be divisible by 3 (since the square of a number not divisible by 3 is not divisible by 3, either), i.e., $m = 3k$ for some integer k. Then $m^2 = (3k)^2 = 3^2 \cdot k^2 = 9k^2$. That is $9k^2 = 3n$, and so $3k^2 = n$. Hence, n is 3 times an integer (namely, 3 times k^2); i.e, n is divisible by 3.

Solution to Problem 24. No. Let c be the largest common factor (greatest common divisor, by another name) of m and r. Then $m = kc$ and $n = lc$, where the numbers k and l have no common factor (other than 1). Now $m^2 = (kc)^2 = k^2 \cdot c^2$ and $n^2 = (lc)^2 = l^2 \cdot c^2$. So the equation $m^2 = 3n^2$ becomes $k^2 \cdot c^2 = 3l^2 \cdot c^2$. One can cancel c^2 on both sides to obtain $k^2 = 3l^2$. The right-hand side here is divisible by 3; so is then the left-hand side. Thus k must be divisible by 3; i.e., $k = 3u$ for some integer u. Then $k^2 = (3u)^2 = 3^2 \cdot u^2 = 9u^2$.

Thus, the equation $k^2 = 3l^2$ becomes $9u^2 = 3l^2$, i.e., $3u^2 = l^2$. So l must be divisible by 3. Thus we concluded that k and l are both divisible by 3. This is a contradiction, since k and l have no common factor. This contradiction means that the starting equation, namely $m^2 = 3n^2$ cannot be true when m and n are nonzero integers (of course, the equation is satisfied when $m = n = 0$.)

Note. If this argument is pursued to its natural conclusion, it shows that $\sqrt{3}$ is irrational.

Solution to Problem 25. Assume, on the contrary, that $\sqrt{3}$ is rational. Then there are integers m and n such that $\sqrt{3} = m/n$. We may assume here that the fraction m/n is irreducible. After squaring the above equation, we obtain that $3 = (m/n)^2$, i.e., that $3 = m^2/n^2$. Multiplying both sides by n^2, we obtain that

$$3n^2 = m^2.$$

The left-hand side here is divisible by 3, so the right-hand side must also be divisible by 3, i.e., m^2 is divisible by 3. This means that m must be divisible by 3, since if a number is not divisible by three, its square cannot be divisible by 3, either. Thus, we have $m = 3k$ for some integer k. Then $m^2 = (3k)^2 = 9k^2$, and so the above equation can be written as

$$3n^2 = 9k^2;$$

after dividing both sides by 3, we obtain that

$$n^2 = 3k^2.$$

The right-hand side here is divisible by 3, and so the left side must also be divisible by 3; i.e., n^2 is divisible by 3. This means that n must be divisible by 3, since, as we mentioned just before, if a number is not divisible by three, its square cannot be divisible by 3, either.

We obtained that both m and n are divisible by 3. Thus the fraction m/n can be reduced (by dividing both the numerator and denominator by 3, contradicting our assumption that the fraction m/n is irreducible. This assumption was based on our main assumption that $\sqrt{3}$ is irrational. Since this latter assumption led to a contradiction, this assumption must be false (a correct assumption, combined with correct arguments, cannot lead to a contradiction – if you carefully check the arguments above, you will realize that all the arguments we used were correct). Thus $\sqrt{3}$ must be irrational, as we wanted to show.

Solution to Problem 26. Assume, on the contrary, that $\sqrt{6}$ is rational. Then there are integers m and n such that $\sqrt{6} = m/n$. We may assume here that the fraction m/n is irreducible. After squaring the above equation, we obtain that $6 = (m/n)^2$, i.e., that $6 = m^2/n^2$. Multiplying both sides by n^2, we obtain that

$$6n^2 = m^2.$$

The left-hand side here is even, so the right-hand side must also be even, i.e., m^2 is even. This means that m must be even, since the square of an odd number is always odd. Thus, we have $m = 2k$ for some integer k. Then $m^2 = (2k)^2 = 4k^2$, and so the above equation can be written as

$$6n^2 = 4k^2;$$

after dividing both sides by 2, we obtain that

$$3n^2 = 2k^2.$$

The right-hand side here is even, and so the left side must also be even; i.e., $3n^2$ is even. Hence n^2 must also be even (the product of two odd numbers is odd; now 3 is an odd number, so if n^2 were also odd, then $3n^2$ would also be odd). This means that n must be even, since, as we mentioned just before, the square of an odd number is always odd.

We obtained that both m and n even. Thus the fraction m/n can be reduced (by dividing both the numerator and denominator by 2, contradiction our assumption that the fraction m/n is irreducible. This assumption was based on our main assumption that $\sqrt{6}$ is irrational. Since this latter assumption led to a contradiction, this assumption must be false (a correct assumption, combined with correct arguments, cannot lead to a contradiction – if you carefully check the arguments above, you will realize that all the arguments we used were correct). Thus $\sqrt{6}$ must be irrational, as we wanted to show.

Note. The above proof showing that $\sqrt{6}$ is irrational is an almost identical copy of the proof that $\sqrt{2}$ is irrational. One can give a slightly different proof by adapting the proof that $\sqrt{3}$ is irrational.

Solution to Problem 27. Assume that $\sqrt{2} + \sqrt{3}$ is rational; that is, for some integers m and n we have

$$\frac{m}{n} = \sqrt{2} + \sqrt{3}.$$

Squaring both sides of this equation, we obtain

$$\frac{m^2}{n^2} = (\sqrt{2} + \sqrt{3})^2 = (\sqrt{2})^2 + 2\sqrt{2} \cdot \sqrt{3} + (\sqrt{3})^2 = 2 + 2\sqrt{2 \cdot 3} + 3 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6},$$

that is

$$\frac{m^2}{n^2} = 5 + 2\sqrt{6}.$$

It is easy to express $\sqrt{6}$ from this equation. We have

$$\sqrt{6} = \frac{\frac{m^2}{n^2} - 5}{2} = \frac{m^2 - 5n^2}{2n^2};$$

the second equality here was obtained by multiplying both the numerator and the denominator of the fraction in the middle by n^2. The right-hand side here is the ratio of two integers, and so it is a rational number. Therefore the left-hand side (being the same number) is also a rational number; i.e., $\sqrt{6}$ is a rational number. This is, however, a contradiction, since we proved earlier that $\sqrt{6}$ is irrational. This contradiction shows that our assumption, namely, that $\sqrt{2} + \sqrt{3}$ is rational, cannot be valid. Thus, $\sqrt{2} + \sqrt{3}$ is irrational, as we wanted to show.

Solution to Problem 28. Assume that B is rational. Then there are integers m and n such that $B = m/n$; we may also assume that the integers m and n are positive, since the number B itself is positive (a negative power of 3 would be less than 1). That is, $3^{m/n} = 10$; in other words,

$$3^m = 10^n.$$

This equation, however, cannot hold with any positive integers m and n; namely, the only prime divisor of the left-hand side is 3, whereas the only prime divisors of the right-hand side are 2 and 5 (the prime divisors of 10). Since this equation cannot hold, the assumption that B is rational is not correct.

Solution to Problem 29. Let m and n be integers, and think about calculating the fraction m/n by long division. When doing the division by n, there can only be n different remainders (namely, 0, 1, 2, $\dots$, $n-1$). Suppose you are at a stage when the digits of m have been used up – i.e., when you attach a zero to the last remainder to continue the division. When, after this point, the same remainder comes up the second time, the digits will repeat.

Solution to Problem 30. Writing $x = 2.124343434\overline{343}$, we have

$$\begin{array}{rr} 100x = & 212.4343434\overline{343} \\ -x = - & 2.1243434\overline{343} \\ \hline 99x = & 210.31 \end{array}$$

Thus

$$x = \frac{210.31}{99} = \frac{21031}{9900}.$$

This fraction may or may not be reduced, but that makes no difference to the argument. What this equation shows is that x equals the ratio of two integers, i.e., that x is a rational number, as claimed.

Solution to Problem 31. Any nonrepeating decimal will do. For example, the numbers

$$0.101001000100001\dots$$

(one, two, three, four, etc 0s inserted between 1s) and

$$0.12345678910111213141516171819202122\dots$$

(the digits are formed by the consecutive integers 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13,...) are irrational. For most irrational numbers, including $\sqrt{2}$ and π, there are no such simple rules describing the digits of their decimal expansions.

Solution to Problem 32. Writing $x = 0.99999\dots$, we have

$$\begin{array}{rr} 10x = & 9.99999\dots \\ -x = & -0.99999\dots \\ \hline 9x = & 9 \end{array}$$

Thus $x = 9/9 = 1$.

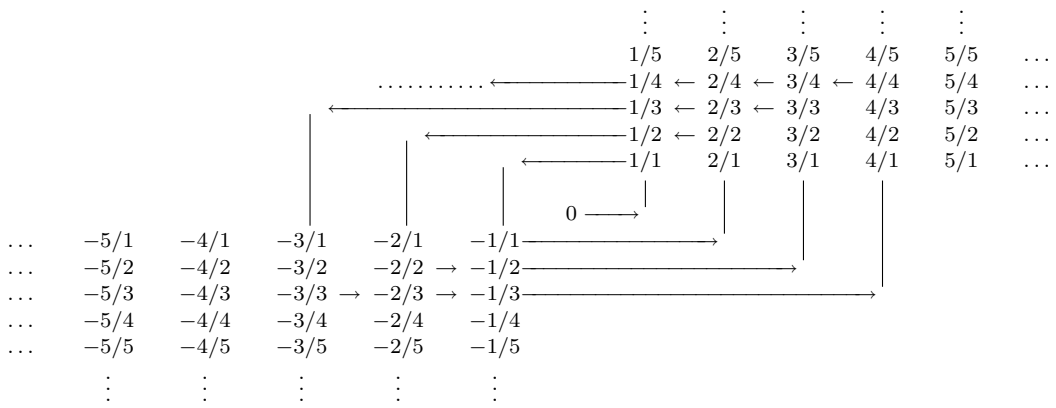
Solution to Problem 33. The correspondence is illustrated by the following diagram:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \dots \\ 2 & 3 & 4 & 5 & \dots \end{array}$$

Solution to Problem 34. The correspondence is illustrated by the following diagram:

$$\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \dots \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & \dots \end{array}$$

Solution to Problem 35. In the diagram



follow the rectangular "spiral" path out from 0, and match up the fractions passed by with the integers 1, 2, 3, 4,..., in turn, omitting those fractions that can be reduced. We obtain the following one-to-one correspondence:

1	2	3	4		5	6		7	8	9		10	...
↓	↓	↓	↓		↓	↓		↓	↓	↓		↓	...
0	1/1	−1/1	2/1	omit 2/2	1/2	−2/1	omit −2/2	−1/2	3/1	3/2	omit 3/3	2/3	...

Solution to Problem 36. We will write down a number that differs from each number in its "diagonal" digit; that is, it will differ from $f(1)$ in its first decimal, from $f(2)$, in its second decimal, from $f(3)$, in its third decimal, from $f(4)$, in its fourth decimal, and so on: $d = 0.2422242\ldots$ (we use d so as to suggest diagonal). In writing down this number, we only use the digits 2 and 4, in order to avoid writing down a number that ends in all 9s, such as $0.235999999\ldots$; this number is equal has two representations, since it is equal to $0.23600000\ldots$ or 0.236.[4] Avoiding numbers with two representations ensures that if two numbers look different, then they are different.

In writing down d, we choose the first decimal of d to be 2, since the first decimal of $f(1)$ is 3, thus ensuring that d differs from $f(1)$; we choose the second decimal to be 4, since the second decimal of $f(2)$ is 2, thus ensuring that d differs from $f(2)$; we choose the third decimal to be 2, since the third decimal of $f(3)$ is 0, thus ensuring that d differs from $f(3)$; we choose the fourth decimal to be 2, since the fourth decimal of $f(4)$ is 4, thus ensuring that d differs from $f(4)$, and so on.

Thus, the real number d is not on the list of real numbers $f(1)$, $f(2)$, $f(3)$, ..., since it is different from each of these real numbers. Hence it is not possible to list all real numbers; i.e., it is not possible to set up a one-to-one correspondence between the set of all real numbers and the set of positive integers. Hence, this argument shows that the cardinality of the set of real numbers is larger than the cardinality of the set of positive integers; that is, that there are more real numbers than there are positive integers.

Solution to Problem 37. In effect we are using the same diagonalization argument that was used in case of the real numbers. We write down a sequence whose elements are different from the diagonal elements of the sequences $f(1)$, $f(2)$, $f(3)$, and so on. We obtain the sequence $d = 0011001\ldots$.

The first element of d is 0, since the first element of $f(1)$ is 1, thus ensuring that d differs from $f(1)$. The second element of d is 0, since the second element of $f(2)$ is 1, thus ensuring that d differs from $f(2)$. The third element of d is 1, since the third element of $f(3)$ is 0, thus ensuring that d differs from $f(3)$. The fourth element of d is 1, since the fourth element of $f(4)$ is 0, thus ensuring that d differs from $f(4)$; and so on.

Thus, the sequence d is not on the list of sequences $f(1)$, $f(2)$, $f(3)$, ..., since it is different from each of these sequences. Hence it is not possible to list all infinite sequences of 0s and 1s; i.e., it is not possible to set up a one-to-one correspondence between the set of all infinite sequences of 0s and 1s and the set of positive integers. Hence, this argument shows that the cardinality of the set of all infinite sequences of 0s and 1s is

[4] One can make the construction of d completely determined by stipulating that one always uses the digit 2 unless one needs to use another digit (if the number $f(n)$ has the digit 2 at the nth decimal place, one needs to use a different digit to ensure that the diagonal differs from $f(n)$), in which case one uses 4.

larger than the cardinality of the set of all positive integers; that is, there are more infinite sequences of 0s and 1s than there are integers.

Solution to Problem 38. We define the set D as

$$D = \{n : n \notin f(n),\ n = 1, 2, 3, 4, \dots\}.$$

This will result in the set

$$D = \{2, 4, 6, 7 \dots\}.$$

We will give some details. 1 is not in D since 1 is in $f(1)$; this ensures that D is different from $f(1)$. 2 is in D since 2 is not in $f(2)$; this ensures that D is different from $f(2)$. 3 is not in D since 3 is in $f(3)$; this ensures that D is different from $f(3)$. 4 is in D since 4 is not in $f(4)$; this ensures that D is different from $f(4)$. 5 is not in D since 5 is in $f(5)$; this ensures that D is different from $f(5)$. 6 is in D since 6 is not in $f(6)$; this ensures that D is different from $f(6)$. 7 is in D since 7 is not in $f(7)$; this ensures that D is different from $f(7)$. 8 is not in D since 8 is in $f(8)$; this ensures that D is different from $f(8)$; and so on.

Thus, the set D is not on the list of sets $f(1)$, $f(2)$, $f(3)$, ..., since it is different from each of these sets. Hence it is not possible to list al subsets of the set of positive integers; i.e., it is not possible to set up a one-to-one correspondence between the set of subsets of the set of positive integers and the set of positive integers. Hence, this argument shows that cardinality of the set of all subsets of the set of positive integers is larger than the cardinality of the set of positive integers. In other words, there are more sets of positive integers[5] than there are positive integers.

Solution to Problem 39. We define the set D as

$$D = \{n : n \notin f(n),\ n = 1, 2, 3, 4, 5\}.$$

This will result in the set

$$D = \{3, 4\}.$$

Since S is a finite set, we can give all the details. 1 is not in D since 1 is in $f(1)$; this ensures that D is different from $f(1)$. 2 is not in D since 2 is in $f(2)$; this ensures that D is different from $f(2)$. 3 is in D since 3 is not in $f(3)$; this ensures that D is different from $f(3)$. 4 is in D since 4 is not in $f(4)$; this ensures that D is different from $f(4)$. 5 is not in D since 5 is in $f(5)$; this ensures that D is different from $f(5)$.

Thus, the set D is not on the list of sets $f(1)$, $f(2)$, $f(3)$, $f(4)$, and $f(5)$, since it is different from each of these sets. Hence it is not possible set up a one-to-one correspondence between the set $S = \{1, 2, 3, 4, 5\}$ and the set of all subsets of this set. Thus, this argument shows that the cardinality of the power set of S is larger than the cardinality of S. That is, the set $S = \{1, 2, 3, 4, 5\}$ has more than 5 subsets. In practice this is not a very exciting result, since it is well known that S has many more than 5 subsets; in fact, it has 32 subsets. The reason we showed this argument for S is that since, S being a finite set, all the details can be concretely written out. In case of an infinite set, the concrete details cannot be given, they can only be imagined.

The practical value of this argument, called *diagonalization*, is for infinite sets, where it is the only way of showing that the power set of an infinite set has a cardinality larger than the set itself.

Solution to Problem 40. Assume that f is a one-to-one[6] mapping os S to $P(S)$; we will exhibit an element of $P(S)$ that is not of the form $f(x)$ for $x \in S$; that is, there is no one-to-one correspondence between S and $P(S)$. The set we will exhibit is the "diagonal"

$$D = \{x \in S : x \notin f(x)\}.$$

Given an arbitrary $x \in S$, the set D is different from the set $f(x)$, since if $x \in f(x)$ then $x \notin D$, and if $x \notin f(x)$ then $x \in D$.

[5] A set of positive integers is a subset of the set of all positive integers. Note that these subsets are usually (but not necessarily) infinite.

[6] The assumption that f is one-to-one, meaning that $f(x)$ and $f(y)$ are different if $x, y \in S$ are different, will not be used.

Solution to Problem 41. If S the set of all sets, then its power set $\mathcal{P}(S)$ must have larger cardinality than S. That is, $\mathcal{P}(S)$ must have more elements than S. This is not possible, since the elements of $\mathcal{P}(S)$ are sets, and every set is an element of the set S (since S is the set of all sets).

This is contradiction, called a paradox, is a very serious problem when discussing sets. In order to avoid the problem raised by this paradox, the *intuitive* approach to set theory is not satisfactory. That is, one needs to set up a rigorous framework that does not allow one to talk about the set of all sets. Such a framework is called *Axiomatic Set Theory*. Axiomatic Set Theory seems to avoid all known paradoxes, but it is *impossible* to prove that new paradoxes cannot arise. It is not only the case that it has not been proved that new paradoxes cannot arise; it has been proved (by Kurt Gödel, and Austrian mathematician in 1931[7]) that it is *impossible to prove* that there are no new paradoxes. An amusing description of the history surrounding this, and its significance for the design of computers, can be found at the Web site

`http://members.cox.net/mathmistakes/greatestmistake.htm`

Solution to Problem 42. Russell defines the set of all those subsets that are not elements of themselves. Formally, Russell's set is defined as

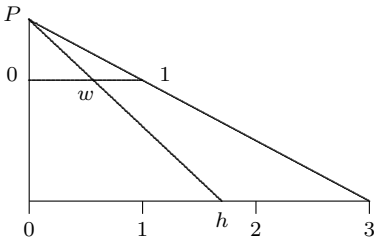
$$R = \{x : x \notin x\}.$$

That this set can lead to difficulties should not be a surprise, because we mentioned that set of all sets already lead to difficulties. Further, it is not clear whether the concept of a set having itself as an element is sound. To know what a specific set is, one has to know all its elements beforehand. But if a set S has itself as an element, how can one know what S is before one forms the set S?

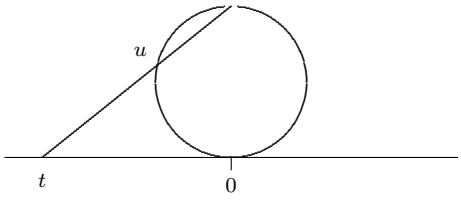
The problems raised by Russell's paradox are more direct than those raised by the set of all sets. Namely, the question whether $R \in R$ cannot be answered. If one assumes that $R \in R$ then the definition of R shows that $R \notin R$ (since taking $x = R$ in this definition, the condition $x \notin x$ is not satisfied). If, on the other hand, one assumes that $R \notin R$ then the definition of R shows that $R \in R$ (since taking $x = R$ in this definition, the condition $x \notin x$ is satisfied).

The difficulty raised by Russell's paradox is apparently avoided in Axiomatic Set Theory; however, one cannot know whether this is in fact the case.

Solution to Problem 43. This can be done simply by projecting one line to the other. In the picture on the right you can see how to project a line segment of length one 1 a line of length 3. The picture shows how a number w in the line segment $(0, 1)$ (the set of all numbers greater than 0 but less than 1) is mapped onto the number h in the line segment $(0, 3)$ by drawing a straight line through the tip of the triangle at P. It is also easy to describe this map algebraically ($h = 3w$ in the present example).



Solution to Problem 44. Take the finite line segment (with the endpoints not included), and roll it up into a circle; the circle will be missing its "North Pole" (its highest point). Then use the stereographic projection to map this circle onto the line. The stereographic projection maps a point of the circle to the line on which the circle is sitting by connecting the point with the North Pole of the circle; the this line will hit the horizontal line at the image of the point on the circle. In the picture on the right, the point u on the circle is mapped to the point t on the horizontal line. The stereographic projection maps every point of the circle (except the North Pole) onto the horizontal line.



Solution to Problem 45. Take the line segment as the part of the number line with numbers between 0 and 1. The square will be represented by pairs of numbers between 0 and 1. Each real number should be represented in a way that a number is not allowed to end in all 0's.[8] A point (x, y) in the square (described

[7] Gödel later settled in Princeton, New Jersey.

[8] Thus, for example, the number 0.73, which would normally be written as $0.73000\ldots$ (with infinitely many zeros, should be written with its alternate representation as $0.72999\ldots$ (with infinitely many 9s).

by two numbers x and y between 0 and 1) are mapped to a number t between 0 and 1 by intermixing the digits of x and y as follows: take groups of digits alternately from x and y to build up the digits of t. Each time, take the smallest group of digits not ending in zero.[9] For example, if

$$x = 0.1400302740000902\ldots \quad \text{and} \quad y = \mathbf{0.0214000392007}\ldots,$$

then first we divide x and y into groups as described:

$$x = 0.\ 1\ 4\ 003\ 02\ 7\ 4\ 00009\ 02\ \ldots \quad \text{and} \quad y = \mathbf{0.\ 02\ 1\ 4\ 0003\ 9\ 2\ 007}\ \ldots.$$

Then, taking groups of numbers alternately from x and y, build up a single number t:

$$t = 0.\ 1\ \mathbf{02}\ 4\ \mathbf{1}\ 003\ \mathbf{4}\ 02\ \mathbf{0003}\ 7\ \mathbf{9}\ 4\ \mathbf{2}\ 00009\ \mathbf{007}\ 02\ \ldots.$$

Observe that if t is given, then x and y can be determined by splitting t into groups, each time, as before, taking the smallest group of digits that does not end in a zero, and putting the groups alternately into x and y.

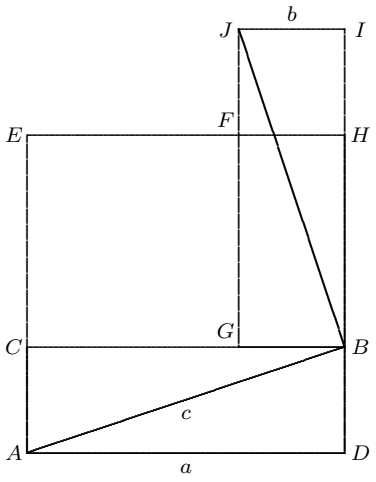
Solution to Problem 46. Consider the unit square, represented by pairs of numbers between 0 and 1, and the unit line segment, represented by single numbers between 0 and 1. One need to ensure that each number only has one representation; for example, never represent a number by digits that are all 0 from some point on.[10] Then there is no pair of numbers (x, y) that corresponds to the number

$$t = 0.420909090909090909\ldots$$

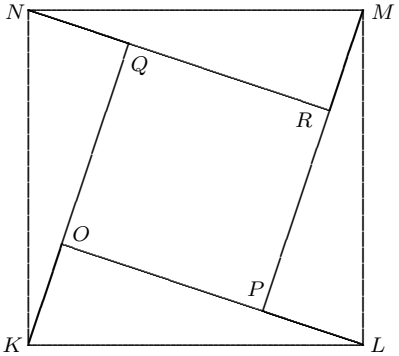
(the number is continued by repeating the groups 09 of digits). Indeed, in order to get t, we would have to have

$$x = 0.400000\ldots \quad \text{and} \quad y = 0.299999\ldots,$$

but $x = 0.400000\ldots$ is not allowed, since a number is not allowed to end in all zeros.[11]



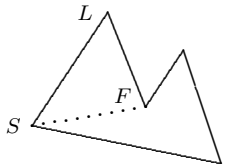
Solution to Problem 47. Consider the two figures. The figure on the left features the triangle ABC with sides $a = BC$, $b = AC$, and $c = AB$. The two squares, $ADHE$ and $FHIJ$ cover an area of size a^2+b^2. This area is made up by four triangles of congruent to the triangle ABC and the square $ECGF$ of side $EC = a - b$. The four triangles and this latter square are rearranged to form the square $KLMN$ on the right, of side $KL = c$. (Note that the small square in the middle, $PRQO$ has side $PO - PL = a - b$, that is, it is congruent to the square $ECGF$ on the left.) The area of the square $KLMN$ is the same as the area on the left covered by the two squares $ADHE$ and $FHIJ$. That is, $c^2 = a^2 + b^2$.



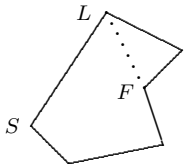
[9] Since we represent a number in such a way that no number ends in all 0s, it is guaranteed that each group of digits is finite.

[10] That is, the number $0.482 = 0.48200000\ldots$ (the number continuing in all zeros) needs to be represented as $0.481999999\ldots$ (the number continuing in all 9s).

[11] If instead of excluding numbers ending in all zeros, we decide to exclude numbers ending in all 9s, then y will become a number that is not allowed.



Solution to Problem 48. We will be able to find a spanning arc unless the floor plan of the art gallery is a triangle. Assume the floor plan is not a triangle, and imagine you are standing at a vertex in a dark art gallery with a flashlight; call this vertex the *flashlight vertex* L (the letters refer to the pictures on the left and the right). You looking at an edge of the gallery. Call the at the far end of this edge the *starting vertex* S (you are standing at the close end L of the edge, with the flash light). Initially, the flash light illuminates the starting vertex S. Move the flashlight until you it illuminates the first vertex (other than the starting vertex). Call this vertex the *found vertex* F.



There are two cases. If the flashlight vertex and the found vertex are connected by an edge of the art gallery, then the line connecting the starting vertex and the found vertex is guaranteed to form a spanning arc (SF in the picture on the left).

If the flashlight vertex and the found vertex are not connected by an edge, then the line connecting the flashlight vertex and the found vertex form a spanning arc (LF in the picture on the right).[12]

Solution to Problem 49. First triangulate the art gallery. Then color the vertices of the art gallery by three colors (red, blue, and green) in such a way that in each triangle there will be one vertex of each color. You start with coloring the vertices of an arbitrary triangle, and then continuing with coloring the vertices of the adjacent triangles. If in a triangle, two vertices have already gotten colors (because these two vertices are in common with the triangle next to it, and that triangle has already been colored), we can choose the third color to paint the third vertex.

Once the vertices of the art gallery have been colored, if we place a camera at vertices of one given color (say red), then these cameras will survey the whole art gallery. This is because there will be a camera in each triangle, and from any vertex of a triangle, the whole triangle can be seen.

The only question that remains is, which at color should the the cameras be places. The answer is: at the color which paints the smallest number of vertices. This color will paint at most $n/3$ vertices; otherwise, each color would paint more than $n/3$ vertices, but then the number of vertices would be more than

$$\frac{n}{3}+\frac{n}{3}+\frac{n}{3}=n.$$

Solution to Problem 50. They are the tetrahedron, the cube, the octahedron, the dodecahedron, and the icosahedron.

The regular tetrahedron has four equilateral triangles as faces. At each vertex, three edges come together.

The cube has six squares as faces. At each vertex, three edges come together.

The regular octahedron has eight equilateral triangles as faces. At each vertex, four edges come together.

The regular dodecahedron has twelve regular pentagons as faces. At each vertex, three edges come together.

The regular icosahedron has twenty equilateral triangles as faces. At each face, five edges come together.

Solution to Problem 51. Given a Platonic solid, the centers of each of the faces can be taken as the vertices as a new solid. These new solid is called the *dual* of the given solid.

The dual of the regular tetrahedron is another regular tetrahedron. The dual of cube is the octahedron, and the dual of the dodecahedron is the icosahedron.

This is all that needs to be remembered, since the dual of the dual of a Platonic solid is (a smaller copy of) the original Platonic solid. That the dual of the octahedron is the cube (since the dual of the cube is the octahedron), and the dual of the icosahedron is the dodecahedron (since the dual of the dodecahedron is the icosahedron).

Solution to Problem 52. There are three different ways.

One is Euler's equation saying that

$$V+F-E=2,$$

[12] In the picture on the right the line SF also forms a spanning arc, but this is not guaranteed to be the case. Under the conditions described, it might happen that SF itself is an edge of the art gallery, in which case SF cannot be taken as a spanning arc.

where V is the number of vertices, F is the number of faces, and E is the number of edges.

For example, for the icosahedron $F = 20$ and $V = 12$.[13] Thus,

$$E = V + F - 2 = 30.$$

Another way is to observe that if each face has s sides, then the number of edges is

$$E = \frac{F \cdot s}{2}.$$

This is because each face is next to s edges, and so F faces give rise to $F \cdot s$ edges. However, each edge is shared between two faces, so this number needs to be divided by 2. Thus, for the octahedron, $F = 8$ and $s = 3$; so

$$E = \frac{8 \cdot 3}{2} = 12.$$

The third way is to note that if at each vertex c edges come together then

$$E = \frac{V \cdot c}{2}.$$

This is because each vertex sits on c edges. Hence the V vertices give rise to $V \cdot c$ edges. However, each edge is shared between two vertices (its two endpoints), so this number needs to be divided by 2. Thus, for the dodecahedron, $V = 20$ and $c = 3$,[14] and so

$$E = \frac{20 \cdot 3}{2} = 30.$$

Solution to Problem 53. Given a regular solid, write E for the number of its edges, F for the number of its faces, and V for the number of its vertices. Let s denote the number of sides of each face, c, the number of edges coming into each vertex. Then we have $E = Fs/2$ and $E = Vc/2$.[15] Hence we have $F = 2E/s$ and $V = 2E/c$. Substituting this into Euler's formula

$$V + F - E = 2,$$

we obtain

$$\frac{2E}{c} + \frac{2E}{s} - E = 2,$$

that is,

$$E \cdot \left(\frac{2}{c} + \frac{2}{s} - 1 \right) = 2.$$

The first factor on the left (that is, E) is positive. For the product to be a positive number (namely, the number 2 on the right-hand side), the second factor must also be positive. That is, we must have

$$\frac{2}{c} + \frac{2}{s} > 1.$$

[13] It may be too much to ask to remember how many vertices the icosahedron has. However, since the icosahedron is the dual of the dodecahedron, the number of vertices of the icosahedron is the same as the number of faces of the dodecahedron; that is, $V = 12$ for the icosahedron.

[14] It may be too much to ask to remember how many vertices the dodecahedron has. However, the dodecahedron, being the dual of the icosahedron, the number of its vertices is the same as the number of faces of the icosahedron; that is, 20. Similarly, the number of edges coming together at a vertex of the dodecahedron is the same as the number of sides of each face of the icosahedron; that is, 3.

[15] To count the number of edges, each face gives rise to s edges adjacent to it, so F faces give rise to Fs edges. Since each edge is shared between the two faces adjacent to it, so this number needs to be divided by 2; that is, $E = Fs/2$. Another way to count the number of edges is to note that if each vertex gives rise to the c edges coming into it, then V vertices give rise to Vc edges. Since each edge is shared between two vertices (its endpoints), this number needs to be divided by 2; that is, $E = Vs/2$.

This inequality can hold only under very narrow circumstances. Namely, we must have $c \geq 3$ (we cannot have only two edges coming into a vertex)[16] and $s \geq 3$ (there is no polygon with only two sides).

As $c \geq 3$, we have $2/3 \geq 2/c$, so the above inequality gives

$$\frac{2}{3} + \frac{2}{s} \geq \frac{2}{c} + \frac{2}{s} > 1,$$

i.e.,

$$\frac{2}{3} + \frac{2}{s} > 1.$$

This gives $2/s > 1 - 2/3 = 1/3$, i.e., $6 > s$. Hence the only possible values for s are 3, 4, and 5.

Similarly, As $s \geq 3$, we have $2/3 \geq 2/s$, and a calculation along the same lines shows that the only possible values for c are 3, 4, and 5.

Hence the only possibilities are $s = 3$ and $c = 3$, which gives the tetrahedron;[17] $s = 3$ and $c = 4$, which gives the octahedron; $s = 3$ and $c = 5$, which gives the icosahedron; $s = 4$ and $c = 3$, which gives the cube; $s = 4$ and $c = 4$, but it fact this is not possible, since $2/c + 2/s = 2/4 + 2/4 = 1$ in this case, whereas the quantity on the left must be greater than one according to our key inequality above. $s = 4$ and $c = 5$ is impossible *a fortiori*;[18] $s = 5$ and $c = 3$ gives the dodecahedron. The remaining cases, $s = 5$ and $c = 4$, and $s = 5$ and $c = 5$ are impossible, since $2/c + 2/s \leq 1$ in these cases.

Solution to Problem 54. First, by a *graph* one means a number of points, called *vertices*, some of which are connected by arcs (or lines), called *edges* (the edges do not have to be straight lines). A graph is called *connected* if you can walk from any vertex to any other vertex by traversing a number of edges. Finally, a graph is called *planar* if you can draw it in the plane without any two edges crossing (that is, the edges are allowed to meet only if they run into the same vertex).

One often draws a nonplanar graph in the plane, but then the edges must cross at some points. Such crossing points, however, must be distinguished from vertices. For example, when verifying that a graph is connected by walking from vertex to vertex, one is not allowed to step from one edge onto another at a crossing point; each edge that is traversed, must be fully traversed from the one vertex at its one end to the other vertex at its other end.

Solution to Problem 55. Writing V for the number of vertices, F for the number of regions (faces), and E for the number of edges, we have

$$V + F - E = 2.$$

Keep in mind that when counting the regions, the region at "infinity" also needs to be counted. That is, a region is a part of the plane completely enclosed by edges that is not cut into parts by other edges, and the region that is outside the graph. Using a geographic metaphor, the inside regions can be called *countries*, and the outside region can be called the *ocean*.

Solution to Problem 56. The formula says that

$$V + F - E = 2,$$

where V denotes the number of vertices, F, the number of regions (faces), and E, the number of edges in a connected graph.

First, the formula is certainly valid for small graphs containing one or two vertices. If a graph contain only one vertex then $V = 1$, there is one region (the ocean), i.e., $F = 1$, and there can be no edges, i.e., $E = 0$.[19] As $1 + 1 - 0 = 2$, the formula $V + F - E = 2$ is true in this case.

---

[16] It should be clear that the number of edges coming into a vertex is the same as the number of faces adjacent to a vertex. A vertex sits at the tip of a pyramid (you can obtain this pyramid by slicing off a small part of the solid containing the vertex), and a pyramid cannot have only two sides.

[17] Once s and c are given, the last displayed equation above determines E, and then the other equations given earlier determine F and V. So, given s and c, all the other quantities are determined.

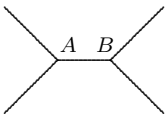
[18] Even more so (because, in this case $2/c + 2/s$ is even smaller, that is $2/c + 2/s < 1$).

[19] Sometimes one allows edges connecting a vertex to itself (such edges are called *loops*). Then $E = 1$; but the loop encloses a region, so $F = 2$. Since $1 + 2 - 1 = 1$, the formula $V + F - E = 2$ is true in this case.

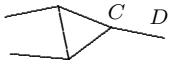
The graph with one vertex is the only one that, strictly speaking, needs to be considered. To feel somewhat more comfortable, one might observe that the formula is also true for a graph with two vertices. In this case $V = 2$. There is still only one region (the ocean), i.e., $F = 1$. There must be one edge, that is, $E = 1$. In fact, if the two vertices were not connected by an edge, then the graph would not be connected, and we are considering only connected graphs, according to the assumptions.

If one is given a larger graph, one can gradually build down, or *deconstruct*,[20] a graph by removing one edge or one vertex at a time, and noticing that one step of such deconstruction will not change the quantity

$$V + F - E = 2.$$



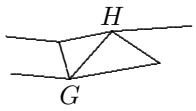
Note that in such deconstruction step, one cannot remove an edge that would make a graph disconnected. For example, in the graph on the right, one is not allowed to remove the edge AB, since this would disconnect the graph.



If in the graph on the left one, removes the vertex D, the number of vertices V decreases by one: $V_{\text{new}} = V - 1$; with the vertex D, one also have to remove the edge CD, since, with the vertex D removed, one end of the edge CD would not be attached to a vertex; so the number of edges also decreases by one: $E_{\text{new}} = E - 1$. On the other hand, the number of faces does not change, so $F_{\text{new}} = F$. Hence

$$V_{\text{new}} + F_{\text{new}} - E_{\text{new}} = (V - 1) + F - (E - 1) = V + F - E.$$

That is, the quantity $V + F - E$ does not change by the removal of a vertex as described.



If in the graph on the right, one removes the edge GH, the number of vertices does not change, that is $V_{\text{new}} = V$. The number of faces decreases by one, that is $F_{\text{new}} = F - 1$. The number of edges decreases by one, that is $E_{\text{new}} = E - 1$. Hence,

$$V_{\text{new}} + F_{\text{new}} - E_{\text{new}} = V + (F - 1) - (E - 1) = V + F - E.$$

That is, the quantity $V + F - E$ does not change by the removal of an edge as described.

Thus, starting with any planar graph, one can build down this graph step by step, by removing an edges and vertices (one at a time), without changing in the quantity $V + F - E$. In a finite number of steps, one arrives at the graph containing one vertex and no edges. Since, as we saw above, in this graph we have $V+F-E = 2$, we must have had $V+F-E = 2$ in the original graph. Thus, Euler's formula is established.[21]

Solution to Problem 57. Place the center of the solid a the center of the sphere, and out of the center of the sphere, project the vertices, edges, and faces of the solid on the sphere. Then take a point on the sphere inside one of the projected faces (so that the point is not at a vertex of on an edge), and use this as the North Pole to project the graph drawn by the projected edges and projected vertices on a plane touching the sphere at the South Pole. We obtain a planar graph; for this Euler's formula $V + F - E = 2$ must hold.[22]

Solution to Problem 58. A pinwheel triangle is a right triangle in which the longer leg[23] is twice as long as the shorter leg. Using the Pythagorean theorem, a simple calculation then shows that the hypotenuse is $\sqrt{5}$ times as long as the shorter leg.

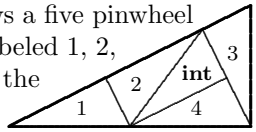
[20] to use a word fashionable in literary criticism.

[21] If one removes the last vertex, one ends up with the empty graph (a vertex with no edges and vertices). One can reasonably say that $V = 0$, $E = 0$, but $F = 1$ in this case, since the whole plane can be considered a single region. In this case, Euler's formula is not valid. If one wants to be overly precise, one should say that Euler's formula holds form *nonempty* connected planar graphs.

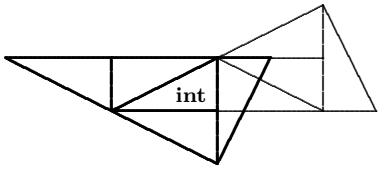
[22] V, F, and E for this planar graph is clearly the same as V, F, and E for the solid we started with.

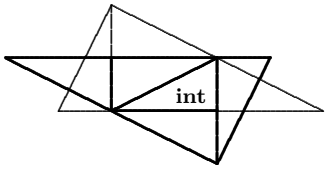
[23] A leg is a side adjacent to the right angle.

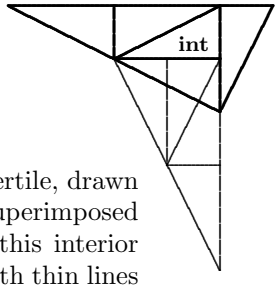
Solution to Problem 59. Consider the figures below: The picture on the right shows a five pinwheel triangles (the tiles), forming a larger pinwheel triangle (the supertile). The tiles are labeled 1, 2, 3, 4, and **int**; the last label refers to the *interior triangle*, and it plays a special role in the considerations involving the pinwheel tiling. It is useful to remember these labels when analyzing the pinwheel tiling.

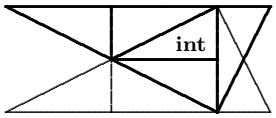


Solution to Problem 60. Consider the figures below:









The figure on left in the top row shows the tiling of a supertile, drawn in thick lines, with the interior triangle labeled as **int**. Superimposed on this, drawn with thin lines, is a supertile that uses this interior triangle as triangle 1. As can be seen, some tiles drawn with thin lines cut some tiles drawn with thick lines, showing that the addition of the tiling drawn with thin lines is not allowed. The figure in the middle in the top row shows what happens if the interior triangle is used as triangle 2 to build a new supertile. Again, tiles are cut. The figure on the on right in the top row shows what happens if the interior triangle is used as triangle 3 to build a new supertile. Again, tiles are cut. The figure on the on left in the bottom row shows what happens if the interior triangle is used as triangle 4 to build a new supertile. Again, tiles are cut.

Solution to Problem 61. The pigeonhole principle says that if we try to put more than n items into n slots (pigeon holes), then there will be one slot that receives more than one of the items.

This is all very simple, and sounds totally harmless. Nevertheless, the pigeonhole principle can be a powerful tool in mathematical arguments where only the existence of an object is proved, while the object itself cannot be identified.

An illustration, silly to the extreme but quite instructive, is the way of showing that there live two persons in the world that have the same number of hairs on their bodies. A fairly routine estimation, not repeated here, shows that no person in the world has more than 400 million hairs. Since there are more than 5 billion people in the worlds, there must be more than one person with the same number of hairs.

What is interesting about this example is that we know for certain that there are two persons in the world with the same exact number of hairs. Yet, there is virtually no chance that we will be able to identify two persons with the same number of hairs.