Solutions to October 2007 Problems

Problem 1. Find all real numbers x such that

$$\sqrt[3]{25+x} + \sqrt[3]{25-x} = 5.$$

Solution. We give several fairly closely related arguments, most fairly closely related. The first one seems unattractive to me, but it is a reasonable approach, and is fairly quick. Rewrite our equation as

$$\sqrt[3]{25+x} = 5 - \sqrt[3]{25-x}. \tag{1}$$

If u and v are real numbers, then $u^3 = v^3$ if and only if $u = v$. So (for real x), by cubing both sides of Equation 1, we obtain the equivalent equation

$$25 + x = 125 - 75(25-x)^{1/3} + 15(25-x)^{2/3} - (25-x),$$

which, after some cancellation, simplifies to

$$(25-x)^{2/3} - 5(25-x)^{1/3} + 5 = 0. \tag{2}$$

Let $y = (25-x)^{1/3}$. We can rewrite Equation 2 as $y^2 - 5y + 5 = 0$, a quadratic equation which has the solutions $y = (5 \pm \sqrt{5})/2$.

So the original equation, as far as solutions in the reals are concerned, is equivalent to $(25-x)^{1/3} = (5 \pm \sqrt{5})/2$. Cube both sides. After some calculation, we arrive at

$$25 - x = 25 \pm 10\sqrt{5},$$

and finally $x = \mp 10\sqrt{5}$. (Yes, it does collapse this much. Could it be trying to tell us something?)

Another Way. The next approach is symmetric and efficient. To make typing easier, and for better reasons, let $a = \sqrt[3]{25+x}$ and $b = \sqrt[3]{25-x}$.

For any a and b, we have

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3 + 3ab(a+b). \tag{3}$$

Identity 3 has a number of uses. It is central in the development of the "Cardano Formula" for the roots of a cubic equation.

Note that for our choice of a and b, we have $(a+b)^3 = 125$ and $a^3 + b^3 = (25+x) + (25-x) = 50$. Substituting in Identity 3, we obtain

$$125 = 50 + 15ab,$$

which yields $ab = 5$. We could go on to find a and b, but there is no need to. Note that

$$ab = \sqrt[3]{25+x}\,\sqrt[3]{25-x} = \sqrt[3]{25^2 - x^2}$$

and therefore $\sqrt[3]{25^2 - x^2} = 5$. Cube both sides. We quickly obtain $x^2 = 500$, so $x = \pm 10\sqrt{5}$.

Comment 1. An important feature of the above argument is that we *preserved* symmetry. The first argument *broke* symmetry. Breaking symmetry is a sin. Like other sins, it can be worth committing, but only if there are clear reasons to do so.

Another Way. Next we give a somewhat less attractive variant of the "nice" argument above. Less attractive it may be, but it introduces some useful ideas. We *factor* $a^3 + b^3$. In general,

$$a^3 + b^3 = (a + b)(a^2 - ab + b^2) \tag{4}$$

Now we can rewrite $a^2 - ab + b^2$ as $(a + b)^2 - 3ab$, which gives

$$a^3 + b^3 = (a + b)((a + b)^2 - 3ab),$$

basically the same result as Identity 3. Substituting in our expressions for a, b, and $a + b$ we find that our equation holds if and only if $50 = 5(25 - 3ab)$, which simplifies to $ab = 5$. Now we can proceed as in the preceding argument.

But if we don't notice that we do not need to calculate a and b, there is a standard way to continue. We know that $(a + b)^2 = 25$. But in general,

$$(a - b)^2 = (a + b)^2 - 4ab.$$

In our case that gives $(a - b)^2 = 5$, so $a - b = \pm\sqrt{5}$ Now that we know $a + b$ and $a - b$, we can calculate a, and if we wish, b. Then we can find x as in the first solution.

Another Way. Let $a-b = w$. Then since $a+b = 5$, we find that $a = (5+w)/2$ and $b = (5-w)/2$. From the fact that $a^3+b^3 = 50$, we get $(5+w)^3+(5-w)^3 = 400$, which simplifies to $250 + 30w^2 = 400$. We conclude that $w^2 = 5$. Now we know $a + b$ and $a - b$, so we can find a and b, and, after a while, x. Or (better) use the fact that $4ab = (a + b)^2 - (a - b)^2$ to find ab. Once we know ab, then, as in the second solution, we can quickly find x.

Comment 2. We sketch an approach which is overkill, but introduces a trick that is useful elsewhere. We use the identity

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca). \tag{5}$$

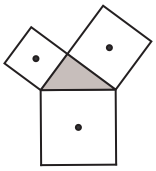
There are nice conceptual proofs of Identity 5. We can also verify it by simply multiplying things out.

In particular, let $a = \sqrt[3]{25 + x}$ and $b = \sqrt[3]{25 - x}$, and let $c = -5$. Then $a + b + c = 0$, and now Identity 5 tells us that $a^3 + b^3 + c^3 = 3abc$. From this we obtain

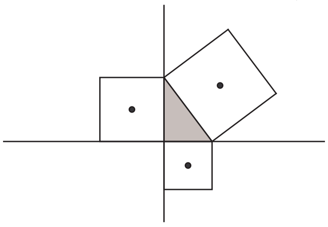
$$(25 + x) + (25 - x) + (-5)^3 = -15\sqrt[3]{25^2 - x^2}.$$

This simplifies to $\sqrt[3]{25^2 - x^2} = 5$, and the rest is easy.

Problem 2. Outward facing squares are erected on the sides of a right-angled triangle whose legs have length a and b. What is the area of the triangle whose vertices are the midpoints of these squares?



Solution. The problem may feel easier if we draw the picture a little differently. Bigger would be nice. It is also good to rotate the diagram as in the picture below. Now draw in the usual x and y axes. So the vertex with the right angle is at the origin, and the other two vertices are at $(a, 0)$ and $(0, b)$.



We compute the coordinates of the centers of the various squares. Two are easy. The square on the side that joins $(0, 0)$ to $(a, 0)$ has coordinates $(a/2, -a/2)$, while the square on the side that joins $(0, 0)$ to $(0, b)$ has coordinates $(-b/2, b/2)$.

Now look at the square on the hypotenuse. The vertex of this square that is nearest $(a, 0)$ is obtained from $(a, 0)$ by going to the right by an amount b, and up by an amount a. So its coordinates are $(a+b, a)$. The center of the square is the midpoint of the diagonal that joins $(a + b, a)$ to $(0, b)$. Thus its coordinates are $((a + b)/2,(a + b)/2)$.

Let ℓ be the line that joins the origin to the midpoint of the square on the hypotenuse. By the calculation of the preceding paragraph, line ℓ has slope 1, so it bisects the right angle. This solves a commonly asked question. As a bonus we find that the line that joins the centers of the other two squares goes through the origin, and is perpendicular to ℓ.

We are almost finished. Our rectangle can be viewed as having "'base" the line segment that joins $(-b/2, b/2)$ to $(a/2, -a/2)$, and height the line segment that joins the point $((a + b)/2,(a + b)/2)$ to the origin. Base and height each have length $(a + b)/\sqrt{2}$, so the required area is $(a + b)^2/4$.

Problem 3. A sequence a, b, c of non-zero real numbers is called a (three-term) *geometric sequence* if $b/a = c/b$. Find all three-term geometric sequences a, b, c such that a, b, and c are integers and $a+b+c = 39$. There is a high probability of missing some sequence(s), so you should *prove* that you got them all—not being able to think of more is not a proof.

Solution. Let me see, the sequence 3, 9, 27 is a geometric sequence ("common ratio" 3) with the right sum. Any others? Of course there is the sequence 27, 9, 3, which is a different *sequence* than 3, 9, 27. The common ratio is 1/3. This "reversing" trick will be useful.

Any others? Here is a boring one: 13, 13, 13. This is certainly a geometric sequence: the defining rule is clearly obeyed, the common ratio is 1. A geometric progression that doesn't progress much! Sadly, the reversing trick gives nothing new.

Any others? Here is a new one: 39, -39, 39 (nobody said all our numbers are positive). The common ratio is -1. Reversing gives nothing new. Any others? Now that we are in a negative mood, maybe we can spot 13, -26, 52. The reversing trick gives 52, -26, 13.

Any others? So far the "common ratio" has been an integer or the reciprocal of an integer. Could it be something else? Our big breakthrough might come when with some playing around, we bump into the sequence 4, 10, 25, which has common ratio $5/2$. Reversing gives 25, 10, 4. Any others? We might notice that $1 - 4 + 16 = 13$. Multiplying through by 3, we get the sequence 3, -12, 48, and, by reversing, 48, -12, 3.

Any others lurking undiscovered? We need to be more systematic if we are to be *certain* that we have them all. Also, we might want to ask the same sort of question for a number other than 39. The following is a systematic approach. The details are not hard. However, maybe it takes a certain amount of experience in number theory to approach things in this way.

Since the terms of our sequence are integers, the common ratio must be a *rational* number. Let it be p/q, where p and q have no factor greater than 1 in common. Without loss of generality we may assume that q is positive. (Note that $p/q = b/a$. To find p and q, we divide each of b and a by the greatest common factor of b and a.)

Our sequence is therefore a, ap/q, and ap^2/q^2. Since p and q have no factor greater than 1 in common, the same is true of p^2 and q^2. And since ap^2/q^2 is an integer, q^2 must divide a. Let $a = dq^2$. Then our sequence is dq^2, dpq, dp^2. The sum is 39, so we arrive at the equation

$$d(p^2 + pq + q^2) = 39 \tag{6}$$

It is convenient, to break the problem into the following cases: (i) $d = 39$; (ii) $d = 13$; (iii) $d = 3$; (iv) $d = 1$.

Case (i): Since $d = 39$, we are looking at the equation $p^2 + pq + q^2 = 1$. For reasons that will become clear soon, we multiply both sides by 4, getting $4p^2 + 4pq + 4q^2 = 4$. Complete the square, and rewrite this last equation as

$$(2p + q)^2 + 3q^2 = 4. \tag{7}$$

Comment 3. It would have been perhaps easier to multiply by 2 instead of 4, and rewrite the equation as $p^2 + q^2 + (p + q)^2 = 2$. This has the advantage of not breaking symmetry. But there are theoretical reasons for preferring the completing the square approach.

Since p and q are non-zero, Equation 7 can only hold if $q = 1$ (since we took q positive) and $2p+q = \pm 1$. Since q is positive, p cannot be positive. So $p = -1$ and $q = 1$. That gives the sequence 39, -39, 39.

Case (ii): Since $d = 13$, we are looking at the equation $p^2 + pq + q^2 = 3$. Multiply through by 4, and rewrite as

$$(2p + q)^2 + 3q^2 = 12. \tag{8}$$

Again we go patiently through the possibilities. We want $12 - 3q^2$ to be a perfect square. That happens at $q = 1$ and $q = 2$.

When $q = 1$, we want $2p + q = \pm 3$. That gives $p = 1$ and $p = -2$. We arrive at the sequences 13, 13, 13 and 13, -26, 52.

When $q = 2$, we want $2p + q = 0$. Thus $p = -1$, and we have the sequence 52, -26, 13.

Case (iii): Since $d = 3$, we are looking at the equation $p^2 + pq + q^2 = 13$. Multiply through by 4, and rewrite the equation as

$$(2p + q)^2 + 3q^2 = 52. \tag{9}$$

We want $52 - 3q^2$ to be a perfect square. That happens when $q = 1$, $q = 3$, and $q = 4$.

If $q = 1$, we want $2p + q = \pm 7$. That gives $p = 3$ and $p = -4$. The geometric sequences are therefore 3, 9, 27 and 3, -12, 48.

If $q == 3$, we want $2p + q = \pm 5$. That gives $p = 1$, and $p = -4$. We get the sequences 27, 3, 1 and 27, -36, 48.

If $q = 4$, we get want $2p + q = \pm 2$. That gives $p = -1$, and $p = -3$, and the sequences 48, -12, 3 and 48, -36, 27.

gap **Case (iv):** Since $d = 1$, multiplying through by 4 as usual we obtain

$$(2p + q)^2 + 3q^2 = 156. \tag{10}$$

We want $156 - 3q^2$ to be a perfect square. That yields the possibilities $q = 2$, $q = 5$, and $q = 7$.

If $q = 2$, we need $2p + q = \pm 12$. Fairly quickly we get 4, 10, 25 and 4, -14, 49. The case $q = 5$ yields 25, 10, 4 and 25, -35, 49. Finally, the case $q = 7$ yields 49, -14, 4 and 49, -35, 25.

By my count, we get a total of 16 solutions! My enumeration was much more tedious than necessary. The situations where $|p| < q$ can be obtained by reversing sequences where $|p| > q$, so the work could have been cut down by almost a factor of two. And there are other shortcuts we could note if the need arose.

Comment 4. This problem, and its relatives, are connected with relatively fancy stuff in Number Theory. The technique we used links the problem with solutions in integers of equations of the shape $x^2 + 3y^2 = 4k$. There is a well worked out theory of this sort of equation, and relatives. The details involve many of the great figures in Number Theory, including Fermat, Euler, Legendre, Gauss, and many others.

As soon as we reached the equation $d(p^2 + pq + q^2) = 39$, the game was for all practical purposes over. For the equation can be rewritten as

$$d(p^2 + q^2 + (p + q)^2) = 78.$$

That forces $|p| < 9$, $|q| < 9$. So immediately we are looking at a smallish number of possible cases. Without loss of generality we can take $q > 1$, and, if we use the "reversing" trick, we can assume that $|p| \geq q$. This cuts down the work quite a bit.

The same problem could be looked at with other numbers than 39. For example, $a + b + c = 91$ gives surprisingly many geometric sequences.

Another Way. We sketch a somewhat different approach, but do not carry out the full details. Let r be the common ratio. Then the terms are a, ar, and ar^2, and our condition is $a(1 + r + r^2) = 39$. The minimum of $1 + r + r^2$ occurs at $r = -1/2$, where $1 + r + r^2 = 3/4$. It follows that $1 \leq a \leq 52$.

Now for every possibility a, solve the quadratic equation $r^2+r+1-39/a = 0$, say by using the Quadratic Formula. We can check easily whether either of the two roots r "works," that is, gives integer values for b and c. A fair amount of work is involved, of course, since at this stage we have 52 candidate values for a. But we *do* get certainty.

There are various ways to cut down on the work. By reversing the sequence if necessary, we can assume that $|r| \geq 1$. That changes the minimum of $1+r+r^2$ to 1, achieved at $r = -1$, and pushes the a we need to look at to the smaller range $1 \leq a \leq 39$.

There is still a lot of effort involved: solving all these quadratic equations is unpleasant. Let's see whether we can do better. Presumably, most r we get will fail to work for the simple reason that they are not even rational. So we can confine attention to the integers a such that

$$r^2 + r + 1 - \frac{39}{a} = 0$$

has a rational root. The above equation has a rational root when the discriminant is the square of a rational number. The discriminant turns out to be

$$\frac{156}{a} - 3.$$

We want this to be the square of a rational. Equivalently (multiply by a^2), we want $a(156 - 3a)$, that is, $3a(52 - a)$, to be the square of a rational (and hence of an integer). It is now possible to scan the various values of a and discard most as candidates. For example, $a = 1$ is no good, we end up with (3)(51), not a square; $a = 2$ is no good, we end up with (6)(50), not a square; $a = 3$ is good, we end up with (9)(49). We then solve $r^2 + r + 1 - 39/3 = 0$, getting $r = 3$ and $r = -4$. Both give suitable sequences, 3, 9, 27 and 3, -12, 48. And $a = 4$ is good. We end up solving the equation $r^2 + r + 1 - 39/4 = 0$. The roots are $r = 5/2$ and $-7/2$. Both give suitable sequences, namely 4, 10, 25 and 4, -14, 49.

Continue, looking at $a = 5$ (no good), 6 (no good), 7 (no good), 8 (no good), and so on. "Most" values of a get easily discarded because the r they give are irrational. It all goes fairly quickly, though if we wanted to, we could invest a bit of thinking into other criteria that eliminate candidates. For example, 5, 10, 15, 20, 30, 35, 40, 45 could not possibly work, since they would give $3a(52 - a)$ which is divisible by 5 but not by 25, and such a thing cannot be a perfect square. Essentially the same remark applies for multiples of 7 that are not multiples of 49, any multiple of 11, and so on. A quick scan shows that the a that work are 3, 4, 13, 25, 27, 39, 48, 49, and 52.

Another Way. As we go systematically through the calculations, particularly in an argument like the first one, maybe we will get the feeling that we are missing something. We are, there is additional algebraic structure in the problem, structure worth exploring. What follows is a rambling exploration, with a number of details not filled in.

Call the elements of our sequence a, ar, ar^2. Now look at the sequence a, $-a(1+r)$, $a(1+r)^2$. This is a geometric sequence with common ratio $-(1+r)$. Add up the terms, first expanding $a(1+r)^2$. A minor miracle happens: The sum is $a + ar + ar^2$! Moreover, if a, ar, and ar^2, then so are a, $-a(1 + r)$, and $a(1+r^2)$. This is clear, let $ar = b$ and $ar^2 = c$. Then $-a(1 + r) = -(a+b)$ and $a(1 + r)^2 = a + 2b + c$.

Another way of putting the same result is to say that if a, b, c is a geometric sequence of the type we are looking for, then so is a, $-(a + b)$, $a + 2b + c$.

So if we find a geometric sequence that works, the above observation gives us another one for free. Is it really another one? Not if the common ratio is unchanged, that is, not if $-(1 + r) = r$. That would give $r = -1/2$. A small calculation shows that we can have $r = -1/2$, in the sequence 52, -26, 13.

Going from r to $-(1+r)$ gives us (almost) a two for one deal. Can we repeat the trick? So we would go from $-(1+r)$ to $-(1+(-(1+r)))$. A lot of brackets, but when the smoke clears, we just have r. This is disappointing, a many for one deal would have been nice. But there is always the old reversing trick.

Start with a positive r. Then $-(1 + r)$ is negative. Do we get all negatives in this way? No, for $-(1+r)$, if r is positive, has absolute value greater than 1. But we do get all negatives with absolute value greater than 1. For look at $-s$, where s is positive and greater than 1. We want to check that $-s = -(1 + r)$ for some positive r. It is, just put $r = s - 1$.

Negatives with absolute value less than 1 could then be dealt with by using the reversing trick. What about the special case where the common ratio is $-s$, where $s = 1$? That comes, in a sense, from $r = 0$. This is not as ridiculous as it looks, the sequence 39, 0, 0 is almost works. It is certainly of the form a, ar, ar^2. We had ruled it out by our *definition.* But the algebra, somehow, would like not to rule it out.

It might be a good idea to listen to the algebra. Euler once remarked (not in English) that “Sometimes my pencil is smarter than I am.” He meant that if a *formal* calculation that doesn’t appear to make much physical sense yields an interesting result, it can still be worth following up.

Back to the listing! Apart from the special case 13, -13, 13, we have seen that every good sequence with a negative common ratio arises through the $-(1+r)$ trick, possibly followed by reversing, from a good sequence with positive common ratio.

The good sequences with positive common ratio are not hard to find. Apart from 13, 13, 13, we can obtain them all by looking at common ratio greater than 1, and possibly reversing. It turns out there are only two, 3, 9, 27 and 4, 10, 25.

They can be found by a crude search. If the common ratio is greater than 1, than we have $b \geq a + 1$, $c > b + 1$. So $3a + 2 < 39$, which tells us that $a \leq 12$. We have $b^2 = ac$, so ac must be a perfect square.

The case $a = 1$ yields the "possibilities" $c = 4$ (ridiculously small), $c = 9$ (ditto), $c = 16$ (which gives $b = 4$, the sum is too small), $c = 25$ (no good, we get sum 31), and $c = 36$ (no good, we get sum 43).

Now look at $a = 2$. To make ac a perfect square, we need an even c. But then b would be even, which is no good, since the sum $a + b + c$ is 39, an odd number. This sort of argument also shows that $a = 6$, 8, and 10 are no good.

Now look at $a = 3$. To make ac a perfect square, c should have the shape $3n^2$. Try $c = 12$, too small. Try $c = 27$, works! There is nothing else to try, the next candidate would be $c = 48$.

Look at $a = 4$. Here c must be a perfect square, indeed an odd one since otherwise $a + b + c$ would be even. Clearly 9 is too small. Try 25; it works!

Look at $a = 5$. Here c should be 5 times a perfect square. Again we could examine cases, there is only one candidate. But let's do it another way, more or less like $a = 2$, 6, 8, 10. If c is 5 times a perfect square, then b also would be, and then $a + b + c$ would be divisible by 5. But 39 is not divisible by 5.

Since $a = 6$ was already dealt with, look at $a = 7$. The argument that took care of 5 deals with this. Or else we can note that the only candidate for c is 28.

The case $a = 9$ is easy, the only candidate for c is 36, giving an $a + b + c$ which is clearly too big. The case $a = 11$ is really easy, there are no candidates for c. That is also true of $a = 12$.

Comment 5. We could have used the "cases" analysis above to deal with negative common ratio, without using the "$-(1 + r)$ trick. But a negative term messes up the kind of quick "too big" judgments that we made, since there could be cancellation.

Divisibility arguments are still quite effective. We can still argue quickly that $a = 2$, 5, 6, 7, 8, 10, 11, 14, 15, 17, 18, 19, ... are no good, in exactly the same way as above. The only a that need to be dealt with are a a perfect square, 3 times a perfect square, 13 times a perfect square, or 39 times a perfect square.

We examine the cases $|r| \geq 1$, and use the reversing trick for the others. It is easy to see that even when r is negative, we must have $1 \leq a \leq 39$. We need to look at $a = 1$, 3, 4, 9, 12, 13, 16, 25, 27, 36, and 39.

The arguments are tedious and repetitive. Look for example at $a = 4$, and negative common ratio (we dealt with the positive case earlier). The candidates for c are the perfect squares only. Note that we will have $b = -\sqrt{ac}$. We can't use even perfect squares for c, for that would make a, b, and c all even, which is impossible. So we examine $c = 9$, 25, 49, 91, and (maybe) so on.

Clearly $c = 9$ doesn't work, and neither does $c = 25$, for that gives $b = -10$. But $c = 49$ works, we get $b = -14$, so $a + b + c = 39$. Do we need to go on? We will show that nothing larger than 7 can work. For if $c = k^2$ with k positive, then $b = -2k$, and $a + b + c = 4 - 2k + k^2$. Rewrite this as $(k - 1)^2 + 3$. If $k > 7$, then $(k - 1)^2 + 3$ is greater than 39. Dealing with the other cases is just as straightforward as the case $a = 4$, usually more so.

Comment 6. In the first solution, we arrived at $a = dp^2$, $b = dpq$, $c = dq^2$. The "$-(1 + r)$" trick transforms this to $a = dp^2$, $b = -dp(p + q)$, $c = (p + q)^2$. This view of things is more symmetric, and therefore can lead to greater progress, and easier computations.

Problem 4. Let α, β, and γ be the angles of a triangle. Can $\tan\alpha$, $\tan\beta$, and $\tan\gamma$ all be integers? A numerical computation can be very useful, but may not be decisive. If a calculator says that the answer is -17, the true answer is (probably) *close* to -17, but may not be exactly *equal* to -17.

Solution. Rename the angles if necessary so that $\alpha \le \beta \le \gamma$. Then $\alpha \le 60°$. We know that $\tan 60°$ is about 1.73. It follows that the only way that $\tan\alpha$ can be an integer is if $\tan\alpha = 1$, that is, α is $45°$.

That leaves 135 degrees to be split between β and γ. But β cannot be 45 degrees, else γ would be 90 degrees, and tan is not defined at $90°$. The tangent of $67.5°$ is about 2.41, which means that the only possibility for $\tan\beta$ is 2. This fixes β: the calculator says that β is about 63.43 degrees. That makes γ about 71.5650511771 degrees.

My calculator says that the tangent of γ is 3. So that's our answer, or is it? We should check that $\tan\gamma$ is *exactly* 3. It is not hard to see that in general $\tan(180 - \theta) = -\tan\theta$. So

$$\tan\gamma = -(\tan(\alpha + \beta)).$$

Recall that in general

$$\tan(x + y) = \frac{\tan x + \tan y}{1 - \tan x \tan y}.$$

Put $x = \arctan 1$, $y = \arctan 2$. We get that $\tan(x + y) = -3$.

Problem 5. For any non-negative integer n, let a_n be the remainder when 2^n is divided by 10000. Show that the sequence a_0, a_1, a_2, and so on is ultimately periodic.

Solution. It is worthwhile to look at much "smaller" problems. For example, use 10 instead of 10000. The successive remainders on division by 10 (that is, the last decimal digits) are easy to find: 1, 2, 4, 8, 6, 2, 4, 8, 6, and so on. Since the last digit of $2x$ is completely determined by the last digit of x, the cycle 2486 must repeat endlessly. The cycle length is 4.

Now use 100 instead of 10000. We are looking at the last 2 digits of 2^n. Calculation gives 1, 2, 4, 8, 16, 32, 64, 28, 56, 12, 24, 48, 96, 92, 84, 68, 36, 72, 44, 88, 76, 52, 04, 08, and so on. The last digit 04 means that the remainder is 4. So the chunk of length 20 that goes from 4 to 52 must repeat endlessly, since the last 2 digits of $2x$ are completely determined by the last 2 digits of x. The cycle length is 20.

Already 100 took some work: 10000 may be much more unpleasant. But note that we are not asked to find the cycle, just to show that there *is* cycling. In what follows, we modify the usual decimal notation a little, by for example writing 0064 instead of 64. This is harmless, and makes the discussion smoother.

Compute. The first few remainders are 0001, 0002, 0004, 0008, 0016, $\dots$, 1024, 2048, 4096, 8192. Then comes 6384, 2768, 5536, 1072, and so on.

It is easy to see that a_n is the number made up by just keeping the "last 4" decimal digits of 2^n. If we know a_n for some particular n, we do not need to know 2^{n+1} in order to find a_{n+1}. If we think about the ordinary process of multiplying by 2, we can see that a_{n+1} is completely determined by a_n. For example, we don't need to know that $2^{14} = 16384$ in order to find a_{15}: we can confine attention to 6384, double that, and keep the last 4 digits.

There is no real saving at $n = 14$. But if we really want to compute for a long time, there is considerable saving by the time n reaches, say, 50. The 2^n become very large, while the a_n stay small.

This is important for more than computational convenience. For imagine, for example, that through a calculation it turned out that $a_{43} = a_{20}$ (it isn't). Then the computation after $n = 43$ would be exactly the same as after $n = 20$: we would have $a_{44} = a_{21}$, $a_{45} = a_{22}$, and so on up to $a_{66} = a_{43} = a_{20}$. But then the game would start all over again, we would have $a_{67} = a_{21}$, $a_{67} = a_{22}$, and so on. From $n = 20$ on we would have cycling with period 23.

Thus if we compute and find *any* two remainders that are the same, that is, if we find an n and a $d > 0$ such that $a_n = a_{n+d}$, then we know there is cycling from a_n on.

We *could* now compute, and hope to bump into a repetition in the sense described above. This procedure could be painful, for the computation may be long. But we are only asked to show that there
emphis cycling, so all we need to show is that there *must* be repetition. There is no need to identify the place where cycling begins, nor the cycle length.

Instead of computing, *imagine* computing a_0, a_1, a_2, and so on up to a_{10000}. We will have computed 10001 remainders. But there are no more that 10000 conceivable remainders, namely 0, 1, $\dots$, 9999. So among a_0, a_1, $\dots$, a_{10000} there must be at least two equal values. More formally, there exist numbers n and d, with $0 \le n < n + d \le 10000$, such that $a_n = a_{n+d}$. It follows that our sequence of remainders is ultimately periodic, with period ≤ 10000.

Comment 7. The period must be much shorter than 10000, since we have many fewer than 10000 possible remainders. Let $n \ge 4$. Then 2^4 divides 2^n. Note that 2^4 also divides 10000. Let us suppose that

$$2^n = 10000q_n + a_n$$

(so q_n is the quotient). Since 2^4 divides 2^n and also divides 10000, it follows that 2^4 divides a_n. Thus from $n = 4$ on, a_n must be divisible by 16. So we can cut down the candidate list to multiples of 16 tht are less than 10000. There are only 625 multiples of 16 between 0 and 9999. It follows that the cycle length must in fact be ≤ 625.

We can do better. For note that a_n cannot be a multiple of 5 (else 2^n would be, but it isn't). Among the multiples of 16 from 0 to 9999, there are 125 multiples of 5. Thus the number of candidates for a_n, when $n \geq 4$, has shrunk to 500, and the cycle length must be ≤ 500.

There is a theorem of Euler that guarantees that indeed 500 is a period, that the remainder when 2^{504} is divided by 10000 is the same as the remainder when 2^4 is divided by 10000. This is easy to verify numerically.

Computing the remainder when 2^{504} is divided by 10000 is not as hard as it sounds. We cannot do it directly with a standard calculator because of the problem of *overflow*: my calculator simply refuses to find 2^{504}. My calculator even has trouble with 2^{30}, since it switches to scientific notation, which is not helpful for our problem.

We can use a standard trick, which in the world of cryptography is of great *practical* importance. Essentially, the trick consists of getting to high powers by repeated squaring, but we will modify the trick a bit. The remainder for 2^{10} is of course 1024. Square this, keep the last 4 digits to get the remainder when 2^{20} is divided by 10000. Multiply by 2^{10}, keep the last 4 digits to get the remainder for 2^{30}. Square, keep the last 4 digits to get the remainder for 2^{60}. Square, multiply by 2^5, and keep the last 4 digits to get the remainder for 125. Square to get the remainder for 250. We are almost there! We can get there much faster if we use the calculator utility that comes with Microsoft Windows, for it will give us directly the full value of 2^{100}. We drop all but the last 4 digits, raise to the power 4, then multiply by 2^4.

So 500 is a period, but it might not be the *smallest* period. There is some important not too hard theory that shows the smallest period must *divide* 500. It turns out that the smallest period actually *is* 500.

Comment 8. Let b and m be positive integers, and let a_n be the remainder when b^n is divided by m. A minor modification of the above argument shows that the sequence a_0, a_1, a_2, and so on is ultimately periodic.

http://www.pims.math.ca/education/math_problems/
http://www.math.ubc.ca/~adler/problems/