Solutions to December 2007 Problems

Problem 1. Which straight lines have exactly one point in common with the circle with equation $x^2 + y^2 = 1$, and have exactly one point in common with the parabola $y = x^2 + 1$?

Solution. Just so we won't forget about them, let's first deal with vertical straight lines. They are "special" in the sense they meet the parabola at 1 point but are not tangent to it. They are also special because they do not have equations of the shape $y = mx + b$.

The geometry is obvious. Any vertical straight line meets the parabola in 1 point. And a vertical straight line (indeed any straight line) meets the circle in exactly 1 point if and only if it is tangent to the circle. That gives us the lines with equations $x = 1$ and $x = -1$.

We now deal with non-vertical lines. Let the line have equation $y = mx + b$. We would like this line to meet the parabola exactly once. The line and parabola meet at the point with x-coordinate equal to s if $s^2 + 1 = ms + b$. The quadratic equation $s^2 - ms + 1 - b$ has exactly 1 solution if and only if the discriminant $m^2 - 4(1 - b)$ is equal to 0.

Similarly, the line and the circle meet at the point with x-coordinate equal to t if $t^2 + (mt + b)^2 = 1$. There is 1 solution precisely if the discriminant $(2mb)^2 - 4(1 + m^2)(b^2 - 1)$ is equal to 0.

The above discriminant equation simplifies substantially, to $m^2 + 1 = b^2$. Now we want to solve the system of simultaneous equations

$$m^2 - 4(1 - b) = 0, \qquad m^2 + 1 = b^2.$$

From the two equations we conclude that $4(1 - b) = b^2 - 1$, and arrive at the quadratic equation $b^2 + 4b - 5 = 0$, which has the solutions $b = 1$ and $b = -5$.

The solution $b = 1$ yields $m = 0$, which gives us the line $y = 1$. It is a correct answer to the question as put, although the "one point" for the circle and the "one point" for the parabola happen to be the same. The solution $b = -5$ yields $m = \pm\sqrt{24}$.

Thus the lines that meet the circle at one point and the parabola at one point have equations $x = 1$, $x = -1$, $x = 0$, $y = \sqrt{24}x - 5$, and $y = -\sqrt{24}x - 5$. The last two seem reasonably plausible from a rough sketch of circle and parabola. It is certainly obvious that there must be symmetry about the y-axis.

Another Way. We can use a more geometric approach to deal with the tangent line to the circle. Suppose this line is tangent to the circle at (p, q). The tangent line is perpendicular to the line joining the center $(0, 0)$ of the circle to the point (p, q) of tangency. This line has slope p/q, so the slope of the tangent line is $-q/p$. (This reasoning is correct only if p and q are non-zero.)

Thus the tangent line at (p, q) has equation of the shape $qy + px = p^2 + q^2 = 1$. Note that the equation $qy + px = 1$ is right even in the cases where the reasoning was not correct, that is, in the cases $p = 0$ and $q = 0$.

To deal with the fact that this line meets the parabola in only 1 point, we pretty much have to use the discriminant (or calculus). From the equations $y = x^2 + 1$ and $qy + px = 1$, we obtain $q(x^2 + 1) + px = 1$. This has 1 solution in 2 cases: (i) If the equation is not really a quadratic equation ($q = 0$); or (ii) If the discriminant $p^2 - 4(q - 1)$ is equal to 0.

Case (i) is easy, we get $p = \pm 1$, so we get the two vertical lines $x = 1$ and $x = -1$. Look now at the discriminant equation $p^2 - 4(q - 1) = 0$. Since $p^2 = 1 - q^2$, we arrive at the equation $5q^2 - 4q - 1 = 0$, which has the solutions $q = 1$ and $q = -1/5$. The possibility $q = 1$ gives $p = 0$, that is, the line $y = 1$. The possibility $q = -1/5$ gives $p = \pm\sqrt{24}/5$, so we can now write down the equations of the lines in these cases.

Problem 2. Find distinct integers m and n such that $2^n - 2^m$ is a multiple of 2008.

Solution. This takes up a theme already explored in the October 2007 problems. Note that $2008 = (8)(251)$. We will find an integer e such that $2^e - 1$ is divisible by 251. It will turn out that $e = 50$ works. Once we know this, we can take $n = 53$ and $m = 3$.

Look at the remainders when 2^i is divided by 251, as i ranges from 0 to 250. Any remainder must lie between 1 and 250. Since there are 251 values of i between 0 and 250, 2 of the remainders must be equal. This means that there are integers j and k, with $0 \leq j < k \leq 250$, such that 2^j and 2^k have the same remainder on division by 251.

It follows that $2^k - 2^j$ is divisible by 251. However,

$$2^k - 2^j = 2^j(2^{k-j} - 1).$$

Since 251 cannot divide 2^j, it follows that $2^{k-j} - 1$ is divisible by 251. So if we take $e = k - j$, then 251 divides $2^e - 1$.

We are some distance from being finished! So far, all we know is that for *some* e in the interval from 1 to 250, $2^e - 1$ is divisible by 251. But we need to *find* such an e. We can search, with the comfortable knowledge that we need not look at more than 250 candidates.

We want an e such that the remainder when 2^e is divided by 251 is 1. Since $256 = 2^8$, the remainder when 2^8 is divided by 251 is 5. It follows that the remainder when $(2^8)^3$ is divided by 251 is 125, so the remainder when $2(2^{24})$ is divided by 251 is 250. This means that 2^{25} is of the shape $251b - 1$. The square of this has the shape $251c + 1$. It follows that the remainder when 2^{50} is divided by 251 must be 1. So we have found an e that works. In fact, it is the smallest positive e such that $2^e - 1$ is divisible by 251.

Comment 1. Note that 251 is prime. The 17th century mathematician Fermat proved a number of results that have a bearing on our problem.

Theorem 1 (Fermat's "Little" Theorem). Let p be any prime, and let a be an integer which is not divisible by p. Then $a^{p-1} - 1$ is divisible by p.

Theorem 2. Let e be the smallest positive integer such that $a^e - 1$ is divisible by m. If $a^n - 1$ is divisible by m, then n is a multiple of e.

In Fermat's Theorem, take $p = 251$ and $a = 2$. We conclude that $2^{250} - 1$ is a multiple of 251. Thus the search for e need not have involved any computation at all! Let e be the smallest positive integer such that $2^e - 1$ is a multiple of 251. The second result now guarantees that e divides 250. So even if we want to find the *smallest* positive e that works, there are not too many candidates.

Problem 3. What is the largest possible common divisor of $n^3 + 1$ and $n^2 - 5$, as n ranges over the integers?

Solution. Suppose that d divides both $n^3 + 1$ and $n^2 - 5$. Then, since

$$n^3 + 1 - n(n^2 - 5) = 5n + 1 \qquad \text{for all } n, \tag{1}$$

it follows that d divides $5n + 1$. Thus d divides $5n + 1$ and $n^2 - 5$, and since

$$n(5n + 1) - 5(n^2 - 5) = n + 25 \qquad \text{for all } n, \tag{2}$$

it follows that d divides $n + 25$. Thus d divides $5n + 1$ and $n + 25$, and since

$$5(n + 25) - (5n + 1) = 124 \qquad \text{for all } n, \tag{3}$$

it follows that d divides 124. Thus nothing *larger* than 124 can divide both $n^3 + 1$ and $n^2 - 5$. However, there is as yet no assurance that we can find an n such that 124 divides $n^3 + 1$ and $n^2 - 5$.

We have shown that if there is such an n, 124 would have to divide $n + 25$. So we look for an n such that 124 divides $n + 25$. It is clear that $n = 99$ works.

Now we can simply calculate. It turns out that with $n = 99$, 124 indeed divides $n^3 - 1$ and $n^2 - 5$. Note that if we do not have an allergy to negative numbers, we can take $n = -25$. Certainly 124 then divides $n+25$. We calculate $n^3 + 1$ and $n^2 - 25$ at $n = -25$, and check that 124 divides both. It is not hard to show that in fact 124 divides both $n^3 + 1$ and $n^2 - 5$ whenever n is of the form $124k - 25$ for some integer k, and for no other values of n.

Alternately, we can check whether the chain of implications that led us to 124 can be reversed. It can. Here are the details. Suppose that d divides 124 and $n + 25$. Then from Equation 3, it follows that d divides $5n + 1$. But then from Equation 2, it follows that d divides $5(n^2 - 5)$. However, since d divides 124, d is not divisible by 5, and therefore d divides $n^2 - 5$. But then from Equation 1, it follows that d divides $n^3 + 1$, and we are finished.

Comment 2. The technique that we used is closely related to the very important *Euclidean Algorithm* for finding the greatest common factor (GCD) of two integers. We are given two integers a_0 and a_1, say both positive, with $a_0 > a_1$. Divide a_0 by a_1, and suppose that the quotient is q_1 and the remainder is a_2. It is easy to verify that an integer d divides both a_0 and a_1 if and only if d divides both a_1 and a_2. If $a_2 = 0$, the GCD of a_1 and a_2 is a_1. Otherwise, divide a_1 by

a_2, obtaining quotient q_2 and remainder a_3. We are now looking for the GCD of a_2 and a_3. Continue until the GCD jumps out.

Here is a short illustrative example. We want the GCD of 124 and 84. Since $124 = 1 \times 84 + 40$, we want the GCD of 124 and 40. Since $124 = 3 \cdot 40 + 4$, we want the GCD of 40 and 4. Since $40 = 4 \cdot 10 + 0$, we want the GCD of 4 and 0. This is clearly 4.

The above numerical example does not do justice to the importance of the Euclidean Algorithm, since it is very easy to find the GCD of 124 and 84 without even writing down anything, by mentally factoring 124 and 84. However, the factorization approach is not practical if we want the GCD of a_0 and a_1, where a_0 and a_1 are large, since factorization of large numbers is in general computationally very difficult. The Euclidean Algorithm remains quite feasible even for extremely large numbers.

The Euclidean Algorithm has come to be of great practical importance, since it is used in many number-theoretic computations, including those needed for some encryption/decryption procedures. You might want to search under the term RSA. The procedure we used is actually more closely connected to the Euclidean Algorithm for *polynomials,*, which proceeds on lines roughly analogous to those for the Euclidean Algorithm for integers.

Problem 4. Let w be the number of "words," all of whose letters are different, over the standard 26-letter alphabet. Examples of such words are w, bza, and kzlfhg—there are much longer ones. Find $w/26!$, correct to 2 decimal places.

Solution. It seems natural to look first at short words, then at longer words. (The term "word" is here used as an abbreviation for "word with all letters different.")

How many 1-letter words are there? Clearly there are 26. How many 2-letter words? The first letter can be chosen in 26 ways. For every such way, there are 25 ways to choose the second letter, for a total of (26)(25) words. How many 3-letter words? The 3-letter words can be made by taking any 2-letter word, and appending a new letter at the end. There are (25)(25) 2-letter words, and each such word can be completed to a 3-letter word in 24 ways, so there are (26)(25)(24) 3-letter words. Continue in this way. The total number w of words is given by

$$w = 26 + 26 \cdot 25 + 26 \cdot 25 \cdot 24 + \cdots + 26 \cdot 25 \cdot 24 \cdots 1. \tag{4}$$

Comment 3. A mathematician might object that we have forgotten the *empty word,* the word that has 0 letters. The empty word is a quite useful concept. In a discussion of the "algebra" of words, it fills a role similar to the role that 0 plays in ordinary arithmetic. But in our particular problem, since there is only one empty word, whether we include it or not makes no appreciable difference to the answer.

Now divide by 26!. It is convenient to reverse the order of summation in Equation 4. After taking care of the cancellations, we find that

$$\frac{w}{26!} = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{25!}. \tag{5}$$

We want to evaluate the right-hand side of Equation 5 correct to 2 decimal places. One way to do this is to calculate every term explicitly, then add up, and report the answer to 2 decimal places. That is very tedious. Instead, we note that the terms on the right-hand side of Equation 5 decrease quite fast. So, maybe, we can just add up the first few terms, and then *show* that the sum of the rest of the terms makes no difference to the 2 decimal place answer.

The term $1/5!$ is somewhat less than $1/100$, and the term $1/6!$ is substantially less, so maybe

$$1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!}$$

will be close enough. A bit of calculation shows that this sum is about 2.7166, so the number we are looking for is greater than 2.7166. The "error" we are making is the sum of the rest of the terms, the ones we have not bothered to add up. We could calculate that "error" exactly, but that would mean adding up the rest of the terms, which is a fair bit of work. So instead we will *estimate* the error.

The first neglected term is $1/6!$. The second neglected term is $1/7!$. Note that this is equal to $(1/6!)(1/7)$. The third neglected term is $1/8!$. This is less than $(1/6!)(1/7)(1/7)$. Similarly, the fourth neglected term is $1/9!$, and it is less than $(1/6!)(1/7)^3$. So the entire neglected part of the sum is less than

$$\frac{1}{6!}\left(1 + \frac{1}{7} + \frac{1}{7^2} + \frac{1}{7^3} + \cdots\right).$$

Note that in the line above, we are, for convenience, summing *forever*.

The infinite geometric series above has, by the usual formula, the sum $1/(1-1/7)$. It follows that the error we make by just computing to $1/5!$ is less than $(1/6!)(7/6)$. This last number is about 0.0016204.

It follows that our original sum is between 2.7166 and 2.7183. In particular, our sum, correct to 2 decimal places, is 2.72.

Comment 4. If we ask the corresponding question for an alphabet that has, say, 50 letter, we get an expression for $w/50!$ which looks much the same as the one above, except that the sum goes to $1/49!$. The argument above shows that the sum is, to 2 decimal places, the 2.72 obtained above.

We may want to look instead at the *infinite* sum

$$1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} + \cdots.$$

This sum is one of the most important numbers in mathematics. It is usually called e, the base for natural logarithms. It is omnipresent, for example, in the calculus. To 31 decimal places, it is equal to

$$2.71828182845904523536028747135 27$$

Problem 5. Let n be a positive integer. Which is bigger, $999^n + 1000^n$ or 1001^n? Give as detailed an analysis as possible.

Solution. The answer is: It depends. Certainly $999^n + 1000^n$ is larger than 1001^n when n is fairly small. And it so happens that 1001^n is (much) larger than $999^n + 1000^n$ when n is large. That is a partial answer. But we need to ask: How small is small? How large is large?

We could work with the expressions as given. But for various reasons it is much better to divide both expressions by 1000^n. For one thing, we may want to do some calculations. If I try to compute something modest like 1001^{34}, my calculator overflows, prints $-E-$, and has to be reset.

Our modified question is then: Which is bigger, 0.999^n+1 or 1.001^n? We can give an immediate partial answer. For example, let $n = 1000$. The calculator gives $1.001^{1000} \approx 2.7169$, and of course $0.999^{1000} + 1$ is quite a bit less than 2, indeed it is about 1.3677. (The fact that 1.001^{1000} is bigger than 2 is obvious even without a calculator. For example we can use the Binomial Theorem.)

As n increases, $(1.001)^n$ increases, and after a while becomes very large, while $0.999^n + 1$ decreases towards 0. (This observation is another side benefit of having divided both original expressions by 1000^n.) So there is a first number N such that 1.001^N is greater than $0.999^N + 1$, and from $n = N$ on, we have $1.001^n > 0.999^n + 1$. The only remaining problem is to locate N. So far all we know is that $N \leq 1000$.

Experimentation with the calculator lets us pin down N quite quickly. After a bit of fooling around we find that $N = 482$.

Another Way. Instead of dividing both expressions by 1000^n, we can divide by 1001^n. So we ask which is bigger,

$$\left(\frac{999}{1001}\right)^n + \left(\frac{1000}{1001}\right)^n \qquad \text{or} \qquad 1.$$

After a while, $(1000/1001)^n$ is smaller than $1/2$, and therefore so is $(999/1001)^n$. It follows that after a while, $999^n + 1000^n$ is smaller than 1001^n. And as n increases, $(999/1001)^n + (1000/1001)^n$ decreases. It follows as in the first solution that there is a smallest integer N such that $(999/1001)^n + (1000/1001)^n < 1$ for every $n \geq N$.

Like in the first solution, it remains to pin down N. This can be done fairly quickly with a simple scientific calculator.

Another Way. Note that 0.999 is approximately equal to $1/1.001$. Indeed $1/1.001$ is approximately 0.999001. We replace 0.999 with $1/1.001$. If 0.999^n+1 is approximately equal to 1.001^n, then we should have

$$\frac{1}{1.001^n} + 1 \approx 1.001^n.$$

Let us check when we actually have *equality*. If we replace the $\approx$ by $=$, and manipulate a little, we obtain the equation

$$1.001^{2n} - 1.001^n - 1 = 0.$$

Let $x = 1.001^n$. The above equation becomes $x^2 - x - 1 = 0$, which has the solution $x = (1 + \sqrt{5})/2$. (For obvious reasons we discarded the negative solution.)

Now we ask when $1001^n = (1+\sqrt{5})/2$. Of course we could fool around with the calculator. But we can get there more directly, using logarithms. Any kind of logarithm will do. We will work with "common" logarithms (to the base 10), because they are more "high school." (Actually, common logarithms are getting more and more uncommon in the real world. Logarithms to the base e (natural logarithms) are far more important, and logarithms to the base 2 are more and more used, because of the pervasiveness of computers.)

Let $\tau = (1+\sqrt{5})/2$. We solve the equation $1.001^t = \tau$. Take the logarithm of both sides. We get

$$t \log 1.001 = \log \tau, \quad \text{or equivalently} \quad t = \frac{\log \tau}{\log 1.001}.$$

The calculator gives $t \approx 481.45239$. Now look at $0.999^n + 1$ and 1.001^n for $n = 481$ (which should be too small) and $n = 482$. It turns out that 481 is indeed too small, and that for $n = 482$ we have that $1.001^n > 0.999^n + 1$. We conclude that $N = 482$.

Comment 5. It was not hard to experiment one's way to an answer, as in the first solution. But the third solution is interesting, particularly because of the cameo appearance of the number τ, which crops up in so many other places in mathematics.

Another Way. We can bring more mathematics to bear on the problem. The discussion is informal.

We use the standard, extremely important fact that as M gets very large, $(1+1/M)^M$ approaches a certain number, whose standard name is e, the base for the *natural logarithms.* This number e is roughly 2.71828. More generally, as M gets very large, $1+x/M)^M$ approaches e^x. At $M = 1000$, $(1+1/M)^M$ is about 2.7169, reasonably close to e,

Let $n = 1000s$, where s is of modest size. Then

$$1.001^n = 1001^{1000s} = (1.001^{1000})^s \approx e^s.$$

Now look at 0.999^n. Use the fact that 0.999 is about 1/1.001. Or else take $x = -1$ and use the fact that if M is large then $(1+x/M)^M$ is close to e^x. We conclude that 0.999^{1000} should be close to e^{-1}. Indeed $0.999^{1000} \approx 0.3677$ while $e^{-1} \approx 0.367879$.

So if s is of modest size, and $n = 1000s$, then 1.001^n is about e^s, and 0.999^n is about e^{-s}. We conclude that $0.999^n + 1$ is about the same as 1.001^n roughly where $e^{-s} + 1 = e^s$.

Multiply both sides by e^s, and rearrange a little. We arrive at the equation

$$e^{2s} - e^s - 1 = 0.$$

Let $v = e^s$. Then the above equation can be rewritten as $v^2 - v - 1 = 0$, and has the solution $v = (1+\sqrt{5})/2$, or more briefly $v = \tau$.

Thus $e^s = \tau$, and therefore $s = \ln \tau$. Calculate. We get

$$s \approx 0.4812118.$$

This tells us that we are looking for the first n such that 1.001^n is greater than $0.999^n + 1$, we should look around 481. But it tells us much more. We could for example ask: What is the smallest n such that 10001^n is greater than $9999^n + 10000$.? The answer is that we should look around 4812.

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