Solutions to April 2007 Problems

Problem 1. Let $f(x) = x^2 + 2x - 1$. Solve the equation $f(f(x)) = f(x)$.

Solution. Calculating $f(f(x))$ is a strategic error. The original problem has structure. Expanding hides that structure, and produces a fourth degree equation whose roots are not at all obvious.

Rewrite our equation as $(f(x))^2 + 2f(x) - 1 = f(x)$, and use the quadratic formula to solve for $f(x)$. We conclude that the equation holds at x if and only if

$$f(x) = \frac{-1 \pm \sqrt{5}}{2}.$$

Now solve the quadratic equations

$$x^2 + 2x - 1 = \frac{-1 + \sqrt{5}}{2} \quad \text{and} \quad x^2 + 2x - 1 = \frac{-1 - \sqrt{5}}{2}.$$

We can add 2 to both sides, making the left-hand side into a perfect square. Or more clumsily we can use the quadratic formula. The roots are

$$-1 \pm \sqrt{\frac{3 + \sqrt{5}}{2}} \quad \text{and} \quad -1 \pm \sqrt{\frac{3 - \sqrt{5}}{2}}.$$

These expressions simplify considerably if we notice that $(1 \pm \sqrt{5})^2 = 6 \pm 2\sqrt{5}$.

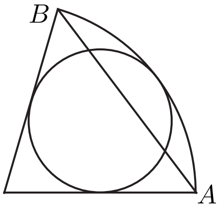
Another Way. Suppose that $f(x) = x$. Apply the function f to both sides. We conclude that $f(f(x)) = f(x)$. So any solution of $f(x) = x$ is a solution of our equation. The equation $f(x) = x$ can be rewritten as $x^2 + x - 1 = 0$, whose roots are $(-1 \pm \sqrt{5})/2$.

Our equation $f(f(x)) = f(x)$ is an equation of degree four, so it has at most 4 roots. To find the other 2 roots, note that $f(x) = (x + 1)^2 - 2$, and therefore $f(-x - 2) = f(x)$ for any x. Thus if $f(x) = -x - 2$ then $f(f(x)) = f(x)$. Now solve the equation $x^2 + 2x - 1 = -x - 2$. The roots are $(-3 \pm \sqrt{5})/2$.

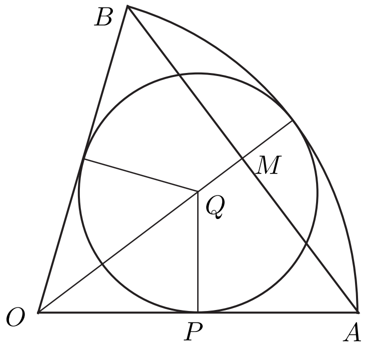
Comment. Both techniques work for *any* quadratic polynomial $f(x)$. If f is any function, a solution of $f(x) = x$ is called a *fixed point* of f. Fixed points are useful in many areas of mathematics.

Problem 2. A circle is inscribed in a sector of a circle, as in the figure below. Suppose that the sector has radius R, the inscribed circle has radius r, and the chord AB has length $2c$. Show that

$$\frac{1}{r} = \frac{1}{c} + \frac{1}{R}.$$



Solution. There is an almost universally applicable rule for problems about circles: the centers are important. So we draw the following picture, where we hope that the meaning of the labelled points is clear.



We have $AM = c$, $OA = R$, $QP = r$, and $OQ = R - r$. But triangles OMA and OPQ are similar. It follows that

$$\frac{OQ}{QP} = \frac{OA}{AM}, \quad \text{that is,} \quad \frac{R-r}{r} = \frac{R}{c}.$$

Divide both sides by R. We obtain

$$\frac{1}{r} - \frac{1}{R} = \frac{1}{c},$$

which is the desired result.

Problem 3. Define the sequence c_0, c_1, c_2, and so on as follows: $c_0 = 2$, and for all non-negative integers n,

$$c_{n+1} = c_n^2 - c_n + 1.$$

(a) Suppose that $d > 1$ and $n > m$. Show that if d divides c_m, then c_n leaves a remainder of 1 when it is divided by d. (b) Use part (a) to show that there are infinitely many primes.

Solution. (a) Suppose first that $n = m + 1$, and let d be a divisor of c_m. Then $c_n = c_m^2 - c_m + 1$. Since d divides c_m, it divides $c_m^2 - c_m$, and therefore $c_m^2 - c_m + 1$ leaves a remainder of 1 on division by d.

Suppose next that $n = m+2$. By the remark above, c_{m+1} leaves a remainder of 1 on division by d. It follows that d divides $c_{m+1} - 1$, and therefore d divides $c_{m+1}(c_{m+1} - 1)$, that is, d divides $c_{m+1}^2 - c_{m+1}$. Thus $c_{m+1}^2 - c_{m+1} + 1$ leaves a remainder of 1 on division by d, so c_{m+2} leaves a remainder of 1 on division by d.

In general, suppose that we know that c_{m+k} leaves a remainder of 1 on division by d. Then, exactly as in the preceding paragraph, d divides $c_{m+k}(c_{m+k} - 1)$, and therefore $c_{m+k}^2 - c_{m+k} + 1$ leaves a remainder of 1 on division by d, that is, c_{m+k+1} leaves a remainder of 1 on division by d, which is what we needed to show.

(b) It is clear that $c_m > 1$ for all m. For any m, let p_m be a prime that divides c_m, say for definiteness the smallest such prime. (It turns out that $p_0 = 2$, $p_1 = 3$, $p_2 = 7$, $p_3 = 43$, and $p_4 = 13$, though these facts are of no importance.)

By part (a), if $n > m$ then c_n leaves a remainder of 1 when it is divided by p_m. In particular, $p_n \neq p_m$. Thus the primes p_0, p_1, p_2, and so on are all *different.* It follows that there are infinitely many primes.

Problem 4. One can find 100 consecutive positive integers none of which is prime. For instance, all of the numbers $101! + 2$, $101! + 3$, $101! + 4$, $\dots$, $101! + 101$ are composite. Show that there are 100 consecutive positive integers among which there are exactly 2 primes. (You will probably not find an *explicit* example—I haven't.)

Solution. For any positive integer n, let S_n be the 100-member set $\{n, n+1, n+2, \dots, n+99\}$. The set S_1 contains lots of primes, 25 I think, S_2 contains 26 primes, while if $n = 101! + 2$, then S_n contains no primes, since for $0 \leq k \leq 99$, the number $n+k$ is divisible by $k+2$, and is clearly (much) greater than $k+2$.

Let $p(n)$ be the number of primes in S_n. There are only 3 possible values of $p(n+1) - p(n)$. Maybe $p(n+1) - p(n) = 1$. This happens if $n + 100$ is prime but n isn't. Maybe $p(n+1) - p(n) = 0$. This happens if n and $n+100$ are both prime or both non-prime. Finally, maybe $p(n+1) - p(n) = -1$. This happens if n is prime but $n + 100$ isn't.

Now look successively at the numbers $p(1)$, $p(2)$, $p(3)$, and so on. As n goes from $n = k$ to $n = k + 1$, $p(n)$ can never decrease by more than 1. Since $p(1) = 25$ and $p(101! + 2) = 0$, it follows that for any integer a between 25 and 0, there must be at least one n less than or equal to $101!+2$ such that $p(n) = a$. In particular there is an n such that $p(n) = 2$.

Comment. We have only given an *existence* proof. I do not know how quickly one can find an explicit example. In searching for one, we would need the help of a *primality testing* program. I recommend the old-fashioned but still useful (and free) language UBASIC, which can do number-theoretic calculations for numbers up to 10^{2000}.

Problem 5. We say that n has been partitioned into almost equal parts if n is expressed as

$$n = a_1 + a_2 + \cdots + a_k,$$

where $k \geq 1$, $a_1 \geq a_2 \geq \cdots \geq a_k$, and $a_k \geq a_1 - 1$. Examples of partitions of 8 into almost equal parts are 8, $4+4$, $3+3+2$, and $2+2+2+1+1$. How many partitions of n into almost equal parts are there?

Solution. We could experiment a bit. There is only 1 partition of 1 into almost equal parts. There are 2 partitions of 2 into almost equal parts, namely 2 and $1+1$. There are 3 partitions of 3 into almost equal parts, namely 3, $2+1$, and $1+1+1$. There are 4 such partitions of 4, namely 4, $2+2$, $2+1+1$, and

$1+1+1+1$. There are 5 such partitions of 5, namely 5, $3+2$, $2+2+1$, $2+1+1+1$, and $1+1+1+1+1$. And without much effort we can find that there are 6 partitions of 6 into almost equal parts, and 7 partitions of 7.

Perhaps the conclusion that there are n partitions of n into almost equal parts becomes quite plausible, or even irresistible. But we should realize that no matter how far we go in our computations, we will only have dealt with a finite number of integers, and there are infinitely many to go. So we need a *proof.*

Let P_n be the set of all partitions of n into almost equal parts. Suppose that someone has listed P_n for us. We show how to produce, with no effort, the set P_{n+1}.

Let p be a partition in P_n. Suppose that all parts of p are equal. For example, we could have $n=6$ and p could be the partition 6, or $2+2+2$. The partition p^* is obtained by adding 1 to the first summand of p. For example, if p is the partition $2+2+2$, then p^* is the partition $3+2+2$, and if p is the partition 6, then p^* is the partition 7.

Suppose that the parts of p are not all equal, as in the partition $2+2+1+1$ of 6. Then p^* is obtained by adding 1 to the first summand of p which is not equal to its predecessor. So if p is $2+2+1+1$, then p^* is $2+2+2+1$.

Thus if p is in turn 6, $3+3$, $2+2+2$, $2+2+1+1$, $2+1+1+1+1$, and $1+1+1+1+1+1$, then p^* is in turn 7, $4+3$, $3+2+2$, $2+2+2+1$, $2+2+1+1+1$, and $2+1+1+1+1+1$.

It is easy to see that every partition in P_{n+1} *except* for the partition $1+1+\cdots+1$ is p^* for some uniquely determined partition in P_n. Thus there is exactly 1 more partition in P_{n+1} than there is in P_n.

Since there is 1 partition in P_1, by the preceding argument there are 2 partitions in P_2, and therefore 3 partitions in P_3, and therefore 4 partitions in P_4, and so on. We conclude that for any n there are n partitions in P_n.

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