# Problem Solving in Math (Math 43900) Fall 2013

Week four (September 17) solutions

Instructor: David Galvin

1. Let $a$ and $b$ be two integer for which $a-b$ is divisible by 3. Prove that $a^3-b^3$ is divisible by 9.

   **Solution**: $a^3-b^3=(a-b)(a^2+ab+b^2)$. Since $a-b$ is known to be divisible by 3, we just need to show that $a^2+ab+b^2$ is too, for the product to be divisible by $3\times 3=9$. We know $a\equiv b \pmod 3$, so (using the basic facts) $a^2+ab+b^2\equiv a^2+a^2+a^2\equiv 3a^2\equiv 0 \pmod 3$; so indeed $a^2+ab+b^2$ is divisible by 3.

   **Source**: Northwestern Putnam preparation.

2. Find all integers $n$ such that $2^n+n|8^n n+n$.

   **Solution**: It seems like, if $2^n+n|8^n n+n$, then the quotient should be something like $n4^n$, so lets hypothesize that it is $n4^n+k$ for some integer $k$. The equation $(2^n+n)(n4^n+k)=n8^n+n$ reduces to $k2^n+n^2 4^n+nk=n$.

   If $k=0$ this becomes $n^2 4^n=n$ or $n4^n=1$. This holds for no $n$.

   If $k>0$, then $k2^n+n^2 4^n+nk>n$, so the equality holds for no $n$.

   If $k<0$, say $k=-\ell$ for $\ell>0$, then the equality becomes

   $$n^2 4^n=(\ell+1)n+\ell 2^n.$$

   For this to hold, we probably need $\ell\approx n^2 2^n$, so try $\ell=n^2 2^n+m$ for integer $m$. The equality becomes

   $$n^3 2^n+mn+n+m2^n=0.$$

   This can't hold for $m=0$ or $m>0$, so consider $m=-k<0$. We reduce to

   $$n^3 2^n+n=k(2^n+1).$$

   The solution to this is probably of the form $k=n^3+r$. Substituting this in leads to

   $$n=n^3+r(2^n+1).$$

   If $r=0$, the only possible solution is $n=1$. If $r>0$, there is no possible solution. If $r=-s$ with $s>0$, then the equation becomes

   $$s(2^n+1)=n^3-n.$$

   It's easy to check that $5(2^n+1)>n^3-n$ for all $n\geq 1$, so we need only consider $s\leq 4$, for which it is easy to check that there are no solution.

So: the only possibility is $n = 1$, which does in fact work, so this is the unique solution.

**Source**: I took this from Northwestern's Putnam preparation, where the original question was to find all $n$ for which $2^n + n | 8^n + n$; using the same strategy this can be solved rather more quickly than the one I (accidently!) wrote.

3. Let $x$, $y$ and $z$ be integers with the property that

$$\frac{1}{x} - \frac{1}{y} = \frac{1}{z}.$$

Prove that both $\gcd(x, y, z)xyz$ and $\gcd(x, y, z)(y - x)$ are both perfect squares.

**Solution**: If we replace $x, y$ and $z$ with $x/\gcd(x, y, z), y/\gcd(x, y, z)$ and $z/\gcd(x, y, z)$ then neither the defining relation, nor the perfect-squareness or otherwise of the targets change, so we might as well assume that $\gcd(x, y, z) = 1$.

So our first task is to show that if $x, y$ and $z$ have no factor in common to all three (other than 1), and $1/x - 1/y = 1/z$, then $xyz$ is a square.

We can get $xyz$ out of the defining relation by multiplying through by $x^2yz$ to get

$$xyz = x^2z + x^y = x^2(y + z)$$

so its enough to show $y+z$ a square. If not, there's some prime $p$ with $p^{2a+1}|(y+z)$, and with $p^{2a+2} \not| (y + z)$. Using $xyz = x^2(y + z)$ we get that $p^{2a+1}|xyz$. But we can't have $p|x$ (we're assuming $\gcd(x, y, z) = 1$), so $p^{2a+1}|yz$. By PHP, we must have either $p^{a+1}|y$ or $p^{a+1}|z$. If the former, then from $p^{2a+1}|(y + z)$ we get $p^{a+1}|(y + z)$ and so $p^{a+1}|z$, and if the latter for the same reason we get $p^{a+1}|y$. So either way, we have *both* $p^{a+1}|y$ and $p^{a+1}|z$, so $p^{2a+2}|yz$, so $p^{2a+2}|(y + z)$, a contradiction. So $y + z$ is a square as required.

Our second task is to show that if $x, y$ and $z$ have no factor in common to all three (other than 1), and $1/x - 1/y = 1/z$, then $y - z$ is a square.

We can get $y - x$ out of the defining relation as follows: multiply through by $xyz$ to get

$$yz = xz + xy$$

which is equivalent to

$$(y - x)(z - x) = x^2.$$

Suppose $p|(y - x)$. Then $p|x^2$ and so $p|x$. Since $p|(y - x)$ we also have $p|y$. Since we are assuming $\gcd(x, y, z) = 1$ we therefore cannot have $p|z$, and so, since $p|x$, we cannot have $p|(z - x)$.

It follows that $\gcd(y - x, z - x) = 1$. How can it be that the product of two numbers is a perfect square ($x^2$ in this case), and the two numbers are co-prime? By looking at the prime factorization, we see that it can happen only if both of the numbers are perfect squares. So $y - x$ is a square, as required.

**Source**: Northwestern Putnam preparation.

4. Let $n > 1$ be an integer and $p$ a prime such that $n|(p-1)$ and $p|(n^3-1)$. Prove that $4p-3$ is a perfect square.

   **Solution**: We have $p|(n-1)(n^2+n+1)$ so either $p|(n-1)$ or $p|(n^2+n+1)$. The first is impossible (it implies $p \leq n-1$, but $n|(p-1)$ says $n \leq p-1$ so $p \geq n+1$). So we have $p|(n^2+n+1)$.

   By $n|(p-1)$ we have $kn = p-1$ for some $k \geq 1$, and by $p|(n^2+n+1)$ we have $\ell p = n^2+n+1$ for some $\ell \geq 1$. From the first, we have $\ell p = \ell kn + \ell$, and so $\ell kn + \ell = n^2+n+1$ or

   $$n^2 + (1-\ell k)n + (1-\ell) = 0.$$

   The solutions to this quadratic must be integers, so the discriminant must be a perfect square, i.e.,

   $$(1-\ell k)^2 - 4(1-\ell) = x^2$$

   for some integer $x$.

   One possibility is $\ell = 1$ (the left-hand side above becomes $(1-k)^2$, certainly a square). But $\ell = 1$ says $p = n^2+n+1$, so $4p-3 = 4n^3+4n+1 = (2n+1)^2$, a perfect square.

   If $\ell > 1$ then rewriting the above as $(\ell k-1)^2 + 4(\ell-1) = x^2$, we see that

   $$4(\ell-1) \geq 2(\ell k-1)+1$$

   (why? $(\ell k-1)^2$ is a perfect square, and when we add $4(\ell-1)$ we get a larger perfect square; the first perfect square after $(\ell k-1)^2$ is $(\ell k)^2$, which differs from $(\ell k-1)^2$ by $2(\ell k-1)+1$, so we need to add at least this much).

   $4(\ell-1) \geq 2(\ell k-1)+1$ implies $k = 1$ (if $k \geq 2$ then $2(\ell k-1) \geq 4\ell-2 > 4(\ell-1)$). But $k = 1$ says $p = n+1$, so $n+1|(n^2+n+1)$, so $n+1|n^2$, impossible for $n > 0$ (why¿ $n+1|n_2-1$, so if $n+1|n^2$ then $n+1|1$).

   **Source**: Northwestern Putnam preparation.

5. Show that the sum of consecutive primes is never twice a prime.

   **Solution**: Suppose $p < q$ are consecutive primes, with $p+q = 2r$ where $r$ is prime. Then $r = (p+q)/2$ satisfies $p < r < q$, a contradiction since there are no primes between $p$ and $q$.

   **Source**: Stanford Putnam preparation.

6. Prove that $2^{70}+3^{70}$ is divisible by 13.

   **Solution**: (Dan's quick solution) $2^2 \equiv -3^2 \pmod{13}$; raising both sides to the power 35, get $2^{70} \equiv -3^{70} \pmod{13}$, and we are done!

   (My laborious solution): By Fermat (or easy multiplication!) we have $2^{12} \equiv 1 \pmod{13}$, so $2^{60} \equiv 1 \pmod{13}$. By easy multiplication, $2^{10} \equiv 10 \pmod{13}$, so $2^{70} \equiv 10 \pmod{13}$.

   By Fermat (or easy multiplication) we have $3^{12} \equiv 1 \pmod{13}$, so $3^{60} \equiv 1 \pmod{13}$. By easy multiplication, $3^{10} \equiv 3 \pmod{13}$, so $3^{70} \equiv 3 \pmod{13}$.

   Combining, $2^{70}+3^{70} \equiv 13 \equiv 0 \pmod{13}$, as required.

   **Source**: Stanford Putnam preparation.

7. Define $f(n)$ by $f(1) = 7$ and $f(n) = 7^{f(n-1)}$ for $n > 1$. Find the last two digits of $f(7)$. (Note that $f(7)$ is an exponential tower of 7's, 7 high.)

   **Solution**: Notice that $7^4 = 2401 \equiv 1 \pmod{100}$. So really all we need to do is to find the remainder, on division by 4, of a tower of six sevens.

   Now $7 \equiv -1 \pmod 4$, and a tower of five 7's is odd, so $f(6) \equiv (-1)^{2k+1} \equiv -1 \equiv 3 \pmod 4$ (here $2k+1 = f(5)$; we don't need to know its value, just that it is odd). So $f(6) = 4m + 3$ for some $m$, and

$$f(7) = 7^{f(6)} = 7^{4m+3} \equiv 7^3(7^4)^m \equiv 43 \pmod{100}.$$

   The last two digits are 43.

   **Source**: Stanford Putnam preparation.

8. Several positive integers are written on a chalk board. One can choose two of them, erase them, and replace them with their greatest common divisor and least common multiple. Prove that eventually the numbers on the board do not change.

   **Solution**: (Thanh's quick solution) If you pick two numbers $a, b$ with $a|b$ or $b|a$, then since $\gcd(a,b) = \min\{a,b\}$ and $\mathrm{lcm}(a,b) = \max\{a,b\}$ in this case, the numbers do not change. In general $\gcd(a,b)|\mathrm{lcm}(a,b)$, so if it is not the case that $a|b$ or $b|a$, then after the swap it *is* the case for that particular pair. Initially there are only finitely many pairs $(a,b)$ with $a \not| b$ and $b \not| a$; either eventually we replace all these pairs with pairs of which one divides to other (in which case we are done), or we eventually commit to avoiding all remaining such pairs (in which case we are done).

   (My laborious solution) When we take a pair of numbers $(a,b)$, and replace them with $(\gcd(a,b), \mathrm{lcm}(a,b))$, we preserve something, namely the product of the pair of numbers (that $ab = \gcd(a,b)\mathrm{lcm}(a,b)$ is easily seen from the prime factorization of $a$ and $b$: if

$$a = \prod_{i=1}^{n} p_i^{a_i}, \qquad b = \prod_{i=1}^{n} p_i^{b_i}$$

   (with maybe some of the $a_i$, $b_i$ zero) then

$$ab = \prod_{i=1}^{n} p_i^{a_i+b_i},$$

$$\gcd(a,b) = \prod_{i=1}^{n} p_i^{\min\{a_i,b_i\}}, \qquad \mathrm{lcm}(a,b) = \prod_{i=1}^{n} p_i^{\max\{a_i,b_i\}},$$

   so

$$\gcd(a,b)\mathrm{lcm}(a,b) = \prod_{i=1}^{n} p_i^{\min\{a_i,b_i\}+\max\{a_i,b_i\}}.$$

   Thus $ab = \gcd(a,b)\mathrm{lcm}(a,b)$ follows from $x+y = \min\{x,y\}+\max\{x,y\}$, valid for any positive integers $x, y$.)

   For any fixed positive number, there are only finitely many ways to write it as the product of a fixed number of positive numbers (if the target of the product is $N$, and we are using $d$ numbers, then each of the $d$ numbers must be a divisor of $N$, so the number of ways of

writing $N$ as a product of $d$ terms is at most $a(N)^d$, where $a(N)$ is the number of divisors of $N$). This shows that there are only finitely many possibilities for the numbers written on the board.

Consider the sum of the numbers. How does this change with the swap operation? It depends on how $a+b$ compares to $\gcd(a,b)+\text{lcm}(a,b)$. Experimentation suggests that $\gcd(a,b)+\text{lcm}(a,b) \geq a+b$, with equality iff the pair $(a,b)$ coincides (in some order) with the pair $(\text{lcm}(a,b), \gcd(a,b))$. To prove this, first consider $a=b$, for which the result is trivial. For all other cases, assume without loss of generality that $a>b$. We have

$$\text{lcm}(a,b) \geq a > b \geq \gcd(a,b).$$

If any one of $a=\text{lcm}(a,b)$, $b=\gcd(a,b)$ holds then by the conservation of product the other must too, and the result we are trying to prove is true. So now we may assume

$$\text{lcm}(a,b) > a > b > \gcd(a,b),$$

and what we want to show is that this implies $\gcd(a,b)+\text{lcm}(a,b) > a+b$. Let $n=ab=\gcd(a,b)\text{lcm}(a,b)$, so

$$\gcd(a,b)+\text{lcm}(a,b) = \gcd(a,b)+\frac{n}{\gcd(a,b)} \quad \text{and} \quad a+b = b+\frac{n}{b}.$$

A little calculus shows that the function $f(x)=x+n/x$ is *decreasing* on the interval $(0,\sqrt{n}]$. Since $\gcd(a,b)<b<\sqrt{n}$, this shows that

$$\gcd(a,b)+\frac{n}{\gcd(a,b)} > b+\frac{n}{b}$$

which is exactly what we want to show.

So, suppose we have the bunch of numbers in front of us, and we perform the swap operation infinitely often. All swaps preserve the product. Some swaps also preserve the sum; these swaps are exactly the swaps that don't change the set of numbers. All other swaps increase the sum. We can only increase the sum finitely many times (there are only finitely many different configurations of numbers). Therefore there must be some point (curiously, not boundable as a function of the original numbers!) after which we make no more sum-increasing swaps; from that point on, the numbers remain unchanged.

**Source**: Stanford Putnam preparation.

9. How many primes numbers have the following (decimal) form: digits alternating between 1s and 0s, beginning and ending with 1?

**Solution**: The number $x_n = 1010\ldots101$, with $n$ 0's, can be written as

$$1+100+1000+1000000+\ldots+1000\ldots000 = 1+(100)+(100)^2+\ldots+(100)^n,$$

in other words, $x_n = P_n(100)$ where $P_n(x)$ is the polynomial $1+x+x^2+\ldots+x^n$.

We want to know for which $n$ the polynomial $P_n(x)$ is prime for $x=100$.

For $n=0$, it is not ($P_0(100)=1$), and for $n=1$ it is ($P_1(100)=101$). So we assume $n \geq 2$.

Since $(x-1)(1+x+x^2+\ldots+x^n)=(x^{n+1}-1)$, we have

$$99P_n(100)=100^{n+1}-1=10^{2(n+1)}-1=\left(10^{n+1}\right)^2-1=\left(10^{n+1}-1\right)\left(10^{n+1}+1\right).$$

What happens if $P_n(100)$ is prime? It must divide one of $10^{n+1}-1$, $10^{n+1}+1$. But, for $n\geq 2$,

$$P_n(100)=1+(100)+(100)^2+\ldots+(100)^n>1+10^{2n}>1+10^{n+1},$$

so $P_n(100)$ is too big to divide either $10^{n+1}+1$ or $10^{n+1}-1$. Hence for $n\geq 2$, $P_n(100)$ can't be prime.

The conclusion is that the only prime of the given form is 101.

**Source**: NYU Putnam preparation.

10. Take a walk on the number line, starting at 0, by on the first step taking a step of length one, either right or left, on the second step taking a step of length two, either right or left, and in general on the $k$th step taking a step of length $k$, either right or left.

    (a) Prove that for each integer $m$, there is a walk that visits (has a step ending at) $m$.

    **Solution**: We can easily get to the number $m=n(n+1)/2$, for any integer $n$: just do $1+2+3+\ldots+n$. What about a number of the form $n(n+1)/2-k$, where $1\leq k\leq n-1$? For $k$ even we can get to this by flipping the $+$ to a $-$ in front of $k/2$. For $k$ odd we can get to this by first adding $n+1$ to the end, then subtracting $n-2$ (net effect: $-1$), then flipping the $+$ to a $-$ in front of $(k-1)/2$.
    Thus we can reach every number in the interval $[n(n+1)/2-(n-1),n(n+1)/2]$. Using $1+2+3+\ldots+n=n(n+1)/2$ we can easily check that the union of these disjoint intervals, as $n$ increases from 1, covers the positive integers. To get to a negative integer $m$, just reverse the signs on any scheme that gets to $-m$.
    Another way to get to $n>0$: do $n=(-1+2)+(-3+4)+\ldots+(-(2n-1)+2n)$.

    (b) Lt $f(m)$ denote the shortest number of steps needed to reach $m$. Show that

    $$\lim_{m\to\infty}\frac{f(m)}{\sqrt{m}}$$

    exists, and find the value of the limit.

    **Solution**: Our second solution to part 1 shows $f(n)\leq 2n$, but to solve part 2 we need to do better. Our first solution to part 1 shows that if $m\in[n(n+1)/2-(n-1),n(n+1)/2]$ then $f(m)\leq n+2$. But it is also easy to see that in that interval, $f(m)\geq n$, since the largest number that can be reached in $n-1$ step is $1+2+\ldots+(n-1)=n(n+1)/2-n$. For $m\in[n(n+1)/2-(n-1),n(n+1)/2]$, we have $(n-1)/\sqrt{2}\sqrt{m}\leq(n+1)/\sqrt{2}$, and so

    $$\sqrt{2}\frac{n}{n+1}\leq\frac{f(m)}{\sqrt{m}}\leq\sqrt{2}\frac{n+2}{n-1}.$$

    Notice that $n$ here is a function of $m$, and that as $m\to\infty$ we have $n\to\infty$ also. So the sequence $f(m)/\sqrt{m}$ is sandwiched between two positive sequences both of which go to $\sqrt{2}$ as $m\to\infty$. By the squeeze theorem,

    $$\lim_{m\to\infty}\frac{f(m)}{\sqrt{m}}$$

    exists and equals $\sqrt{2}$.

**Source**: From *A Mathematical Orchard, Problems and Solutions* by Krusemeyer, Gilbert and Larson.