MA357, Spring 2020 — Problem Set 1 Solutions

1. Prove from the axioms that if $a \in \mathbb{Z}$ and $a \neq 0$, then $a^2 \in \mathbb{N}$. In other words, every nonzero square is positive.

If $a \in \mathbb{N}$ then $a^2 \in \mathbb{N}$ because $\mathbb{N}$ is closed under the operations. If $a \notin \mathbb{N}$ then $-a \in \mathbb{N}$ by trichotomy and $a^2 = (-a)(-a) \in \mathbb{N}$ by closure.

2. NTG, Exercise 2.11.2.

Suppose $a \in \mathbb{N}$, $b \notin \mathrm{N}$. Then either $b = 0$ or $-b \in \mathbb{N}$. If $b = 0$ then $ab = 0 \notin \mathbb{N}$. If $-b \in \mathbb{N}$ then $a(-b) \in \mathbb{N}$ by closure, so $-(ab) \in \mathbb{N}$; by trichotomy, $ab \notin \mathbb{N}$.

3. NTG, Exercise 2.11.9. (Induction practice.)

(1) This one is easy, since factorials are made-to-order for induction.

If $n = 1$ then $n! = 1 = n^n$. Assume that the result holds for $n = k$, so $k! \leqslant k^k$. Since $k < k+1$ we have $k^k < (k+1)^k$, so we have $k! < (k+1)^k$. Now multiply both sides by $k+1$ to get $(k+1)! < (k+1)^{k+1}$.

(2) This one, on the other hand, is quite hard.

If $n = 1$ then $(n+1)^{n-1} = 2^0 = 1$ and $n^n = 1$ as well, so the base case is true. But at first glance it's hard to see how to make the induction work, because powers of $(n+1)$ and powers of $(n+2)$ are not inductively related (i.e., you can't get from one to the other in any sort of easy way). So we need to find a trick.

The idea is to recast what we want to prove into a form friendlier to induction. That's easier said than done: I fooled around for quite a while before I found something that works. We want to prove

$$(n+1)^{n-1} \leqslant n^n$$

It would be better to have $(n-1)$th powers on both sides, so rewrite this as

$$(n+1)^{n-1} \leqslant n^{n-1} n$$

and now we can divide by n^{n-1} to get

$$\left(\frac{n+1}{n}\right)^{n-1} \leqslant n$$

or

$$\left(1+\frac{1}{n}\right)^{n-1} \leqslant n.$$

This we can prove by induction, because $1 + \frac{1}{n+1} \leqslant 1 + \frac{1}{n}$. If we assume it is true for n, then

$$\begin{aligned}\left(1+\frac{1}{n+1}\right)^{n} &= \left(1+\frac{1}{n+1}\right)^{n-1}\left(1+\frac{1}{n+1}\right)\\ &\leqslant \left(1+\frac{1}{n}\right)^{n-1}\left(1+\frac{1}{n+1}\right)\\ &\leqslant n\left(1+\frac{1}{n}\right) = n\cdot\frac{n+1}{n} = n+1.\end{aligned}$$

But! The whole thing is pretty silly, in a way. Induction is far from being the easiest way to prove this. Here are two other approaches that work fine:

a. Let $f(x) = x^x - (x+1)^{x-1}$. Then $f(1) = 0$. Compute $f'(x)$ and check (for example, by plotting it) that it is positive for all $x \geqslant 1$. So $f(x)$ is increasing, so $f(n) > 0$ for all $n \geqslant 2$. In fact, $f(n) \to \infty$ as $n \to \infty$, that is, the inequality is very weak.

b. Remember that $\left(1+\frac{1}{n}\right)^n \to e$ as $n \to \infty$, and in fact it converges from below. (To prove that, expand with the binomial theorem and compare to the series for e.) Since $1 + \frac{1}{n} > 1$, this says

$$\left(1+\frac{1}{n}\right)^{n-1} < \left(1+\frac{1}{n}\right)^{n} < 3,$$

and then we can check for $n = 1$ and $n = 2$ to finish the proof.

4. We say an integer d *divides* an integer n if there exists another integer m such that $n = dm$. Notice that this definition does *not* use the notion of "division," which is right since our axioms don't furnish us with a division operation. In symbols, we write $d|n$ to say "d divides n." That's a vertical bar, not a slash as in a/b, which means "a divided by b".

Let d, m, n, k be integers. Prove following assertions about divisibility. (Most of these are quite easy.)

a. We have $\pm 1|n$ and $\pm n|n$.

   $n = (\pm 1)(\pm n)$.

b. If $d|n$ and $n|m$, then $d|m$.

   Since $d|n$, $n = dx$ for some $x \in \mathbb{Z}$. Since $n|m$, $m = ny$ for some $y \in \mathbb{Z}$. Plugging in, $m = ny = dxy = d(xy)$, so $d|m$.

c. If $d|n$ and $d|m$ then $d|(n+m)$.

   Suppose $d|n$ and $d|m$. By the definition, there exist integers x and y such that $n = dx$ and $m = dy$. But then $n + m = dx + dy = d(x+y)$. Since we know $x + y \in \mathbb{Z}$, we see that $d|(n+m)$.

d. If $d|(n+m)$ and $d|n$ then $d|m$.

   Exactly the same argument: we have $n+m = dx$ and $n = dy$, from which we see that $m = (n+m) - n = d(x-y)$, and certainly $x - y \in \mathbb{Z}$, so $d|m$.

e. If $d|n$ then $d|mn$ for any m.

   We have $d|n$, so $n = dx$ for some x. But then $mn = dxm = d(xm)$, so $d|mn$.

f. If $d|n$ and $d|m$ then $d|(rm + sn)$ for all $r, s \in \mathbb{Z}$.

   Use (e) twice, then (c).

g. For every $k \neq 0$, we have $k|0$ but $0 \nmid k$. (As usual, crossing the symbol means negation, so this says "0 does not divide k.")

$0 = k0$ shows that $k|0$. If k is not zero there is no x such that $k = 0x$, so $0 \nmid k$.

h. If $k|1$, then $k = \pm 1$. (You'll need to use the fact that 1 is the smallest element of $\mathbb{N}$.)

Suppose $1 = kx$. First of all, we know k is not zero. Next, since $kx = (-k)(-x)$, if k is a divisor, then so is $-k$.

So we want to show that any positive divisor must equal 1. Assume k is positive, in which case so is x. Since 1 is the smallest positive number, either $k = 1$ or $k > 1$. But if $k > 1$, $kx > x \geqslant 1$, so in particular $kx > 1$. Hence we must have $k = 1$ if k is positive, $k = -1$ if k is negative.

i. If $m|n$ and $n|m$, then $m = \pm n$.

We have $n = mx$ and $m = ny$. Substituting one into the other we get $n = nyx$. If $n = 0$, then it's clear that $m = 0$. Otherwise, we can cancel n to conclude that $yx = 1$. From the previous result, $y = \pm 1$ and so $m = \pm n$.

5. NTG, Exercise 2.11.15.

The difference between two numbers is divisible by 100 when their last two digits are the same. Since we are supposed to use the pigeonhole principle, that's a clue: we should put two numbers in the same box when the last two digits of their squares are the same.

That makes 100 boxes, alas, any we are only given 52 things to put into the boxes. But remember it is the *squares*! Not all pairs are digits are possible for squares.

How do we find which ones can happen? Essentially by noticing that if two numbers have the same two last digits so do their squares: if

$$a = 100k + n \text{ and } b = 100\ell + n$$

with $0 \leqslant n \leqslant 99$, then

$$a^2 = 100(100k^2 + 2kn) + n^2 \text{ and } b^2 = 100(100\ell^2 + 2\ell n) + n^2,$$

so both a^2 and b^2 have the same last two digits as n^2. I don't want to think too hard, so we could run to GP and type

```
gp > for(n=1,99,print(n^2%100))
```

To get all possible numbers. That gives a list, but I don't care about the list, just about counting them. How many are there? Well, there's a trick: $(100-n)^2 = 100(100-2n)+n^2$ has the same last two digits as n^2. So that means that

$$0^2, 1^2, \ldots, 50^2$$

already gives all possible last two digits. There are 51 numbers on that list. (By homework theory, we should have expected that: otherwise why would be problem say 52 numbers?) OK, we have 52 numbers and 51 boxes, so two of the numbers are in the same box, so their squares end with the same two digits, so the difference of their squares is divisible by 100.

If you do run the GP command, you see that the possible digits are actually

$$\{00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96\}$$

There are only 22 possibilities, which shows that 52 can be replaced with 23... but it makes the problem harder.

6. An integer $n \in \mathbb{Z}$ is called *prime* if it has exactly four divisors, which, by the previous problem, will have to be ± 1 and $\pm n$. (Note that 1 and -1 are not prime, since they have only two divisors. Note also that 0 is not prime.) An integer $n \in \mathbb{Z}$ is called *composite* if it is neither zero, nor ± 1, nor a prime. Prove that if $n \in \mathbb{Z}$, $n \geqslant 2$, then there exists a prime number p such that $p|n$.

The easiest proof is by complete induction. Clearly 2 is divisible by 2, so the base case is true.

Suppose the result is true for all integers a such that $2 \leqslant a \leqslant k$.

Let $n = k+1$. If n is prime, then since $n|n$ we can take $p = n$ and the theorem is true. If not, we know that $n = ab$ with neither a nor b equal to $\pm n$ or ± 1. Since n is positive we can assume a and b are positive. Then we must have $2 \leqslant a \leqslant k$. By the induction hypothesis there is a prime p such that $p|a$. Since $n = ab$, it follows that $p|n$ as well.

7. In a long corridor at the High School in Metropolis, there are $10,000$ lockers in a row, all closed. Then $10,000$ students walk by, and do the following:

- The first student opens all the lockers.
- The second student closes every second locker. (So now locker 1 is open, 2 is closed, 3 is open, etc.)
- The third student changes the state of every third locker: if it is open, she closes it, if it is closed, she opens it.
- The fourth student changes the state of every fourth locker.
- And so on, until the $10,000$th student changes the state of the $10,000$th locker.

At the end of the process, which lockers are open?

(Note that a good solution to this is one in which the number $10,000$ is irrelevant, that is, one that would work just as well if there were 10^{12} lockers.)

The first thing to notice is that the lockers that are open at the end are exactly those whose numbers have an odd number of divisors, since the d-th student changes the state of the n-th locker exactly when $d|n$.

So it boils down to deciding which numbers have an odd number of divisors. But divisors come in pairs: if $d|n$, then $n = dx$ and x also divides n. The only case in which this does not yield two distinct divisors is when $d = x$, that is, when $n = d^2$ is a square. Since in all other cases the divisors come in pairs, the squares are exactly the numbers which have an odd number of divisors. Hence lockers $1, 4, 9, 16, 25$, etc. are the ones that are open at the end.

8. Use the division theorem with $q = 4$ to show that 19 cannot be written as the sum of two squares. (Of course this can be done easily with a brute force search as well, but see the next question.) Can $1,871,266,191$ be written as the sum of two squares? Can you state a general theorem?

The idea is to exploit the uniqueness of the remainder.

When we divide an integer by 4 we get $4q + r$ with $r = 0, 1, 2, 3$.

a. If $n = 4q$, then $n^2 = 16q^2 = 4(4q^2)$ has remainder 0.

b. If $n = 4q+1$, then $n^2 = 16q^2+8q+1 = 4(4q^2+2q)+1$ has remainder 1.

c. If $n = 4q+2$, then $n^2 = 16q^2+16q+4$ has remainder 0.

d. If $n = 4q+3$, then $n^2 = 16q^2+24q+9 = 4(4q^2+6q+2)+1$ has remainder 1.

So any square has remainder 0 or 1. Now

a. $4q+4q' = 4(q+q')$ has remainder 0.

b. $4q+(4q'+1) = 4(q+q')+1$ has remainder 1.

c. $(4q+1)+(4q'+1) = 4(q+q')+2$ has remainder 2.

So the sum of two squares always has remainder 0, 1, or 2. Since $19 = 16+3$ has remainder 3, it cannot be equal to the sum of two squares. The same applies to $1,871,266,191$, which also has remainder 3 (just divide!). The general theorem is: if the remainder of n after division by 4 is $r = 3$, then n cannot be written as the sum of two squares.