MA357, Spring 2020 — Problem Set 1

This assignment is due on **Friday, February 14**. Most of the problems have to do with the axioms for $\mathbb{Z}$ and with divisibility. I will use NTG to refer to our textbook, *Number Theory and Geometry*.

At the end of the problem set there is a problem marked "To Explore." It is not part of the problem set, but it is something interesting you might want to think about.

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.

2. NTG, Exercise 2.11.2.

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

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 $\pm n|n$.

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

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

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

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

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

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.")

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

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

5. NTG, Exercise 2.11.15.

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 $p|n$.

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.)

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?

To Explore: In many parts of the ancient world, fractions were expressed in the following manner. Given any positive rational number x, people would express in a way equivalent to

$$x = n + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_k},$$

where $n, a_1, a_2, \ldots, a_k \in \mathbb{Z}$, $n \geqslant 0$ and $2 \leqslant a_1 < a_2 < \cdots < a_k$. (In particular, repeated denominators were not allowed.) For example, the fraction we know as $\frac{2}{5}$ was given as $\frac{1}{3} + \frac{1}{15}$. Such representations were used in Ancient Egypt, so they are often referred to as "Egyptian fractions."

Explore this idea. Can you prove such a representation always exists? If so, is there an algorithm to find it? Are such representations unique? If they are not unique, it there a way to choose an optimal one?