MATH 8: ASSIGNMENT 20

MARCH 10, 2018

1. Numbers!

One of the most fascinating things about math is the diversity of interesting (and sometimes bizarre) properties that can arise from what looks, at first sight, to be a simple concept - counting numbers 1, 2, 3, ...

As we keep adding 1 we keep getting a new number, which is in a sense its own concept, marking a count of some collection of objects (or however you wish to interpret the number). These numbers are called the natural numbers (sometimes *positive integers*), but some seemingly natural properties of the natural numbers can change dramatically by just adding 1. Take, for example, the concept of dividing numbers. We can arrange 4 dots into a 2x2 square or 6 dots into a 2x3 square, but such a decomposition is not possible for every number. You have probably heard of the concept of a prime number: one which cannot be expressed as a product of two strictly smaller natural numbers; equivalently, we say a number n has a divisor d if we can write n as a product $n = dk$ for k some natural number, then a number p is prime if its only divisors are 1 and p.

Is there an easy way to describe which natural numbers are prime? Or, if I give you an arbitrary natural number and tell you what the two nearest prime numbers are to that number (not including itself), can you tell me if that number is prime? These questions are easy if we ask about the concept of even numbers, for example, but much more deep (and, in many ways, still unsolved) for primality.

So we begin with some concepts: Given natural numbers m, n, we say

- d is a divisor of m, or $d|m$, if $m = dk$ for some natural number k;
- d is a common divisor of m, n if $(d|m) \wedge (d|n)$;
- d is the greatest common divisor of m, n, written $d = gcd(m, n)$ or $d = (m, n)$, if d is greater than or equal to every common divisor of m, n;
- m is prime if $d|m \implies (d = m \vee d = 1)$;
- m is composite if it is not prime;
- m, n are relatively prime if $gcd(m, n) = 1$;
- l is a common multiple of m, n if $(m|l) \wedge (n|l)$;
- l is the least common multiple of m, n, written $l = lcm(m, n)$, if l is less than or equal to every common multiple of m, n;
- p is a prime factor of m if $p|m$ and p is prime.

Some other concepts are common enough to have names, for example: we say that a number is even if it is divisible by 2, and odd otherwise. Typically 2 is defined as 1+1, and 1 is taken for granted (e.g. as an axiom). In this way, one can formally define natural numbers and addition by thinking of all numbers as composites of 1 (i.e., 3 = 1+1+1, 4 = 1+1+1+1, etc.), and multiplication via the $1 \cdot 1 = 1$ and distributive properties ($2 \cdot 2 = (1 + 1)(1 + 1) = 1(1 + 1) + 1(1 + 1) = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 =$ 1+1+1+1).

We'll continue on our journey through numbers with the following theorems, which have interesting ramifications:

Theorem 1. *If $d|m$ and $d|n$ for some numbers d, m, n, then $d|(m - n)$ and $d|(m + n)$.*

Proof. Let $m = ad$ and $n = bd$. Then $m - n = ad - bd = d(a - b)$ and similarly $m + n = d(a + b)$. Since $a - b$ and $a + b$ are natural numbers, we deduce that $m - n$ and $m + n$ both have d as a divisor. □

Theorem 2. *If d is a common divisor of m, n, then for any integers x, y, we have $d|(xm + yn)$.*

Proof. Let $m = ad$ and $n = bd$. Then $xm + yn = xad + byd = d(xa + by)$. □

The following concept is known as *division with remainder*. Can you guess why?

Theorem 3. *Let m, n be natural numbers. Then there exist unique natural numbers q, r, such that $r < n$ and $m = qn + r$.*

The next theorem relates to a concept named after Euclid. The idea is that, if we subtract numbers to get smaller numbers, such a process must end at some point (we cannot have an infinite sequence of decreasing natural numbers). So:

Theorem 4. *For any m, n, $gcd(m, n) = gcd(m, m - n)$.*

Proof. Let $d = gcd(m, n)$. From Theorem 1, we have that $d|m \wedge d|n \implies d|(m - n)$, so d is a common divisor of m, $m - n$. If d were not the greatest common divisor, then there is a larger common divisor e of m, $m - n$, thus by Theorem 1, e is a divisor of $m - (m - n) = n$ and hence e is a common divisor of m, n. But then e is a common divisor of m, n which is larger than d, which cannot happen. Thus d must be the greatest common divisor of m, n. □

Can you guess how this theorem can be used to find the gcd of m, n?

Finally we end on a theorem that might suggest, at least in part, why a greatest common divisor is special.

Theorem 5. *If $d = gcd(m, n)$ and e is a common divisor of m, n, then $e|d$.*

2. Homework

1. If $d|m$, must $d|2m$? What about am for other natural numbers a?
2. Prove that if d is a common factor of m, n, then it is a factor of any common multiple of m, n.
3. If $a|b$ and $b|c$, must $a|c$?
4. Prove that the product of two prime numbers is not prime. Can the product of two composite numbers be prime?
5. If p is prime, how many divisors does p^2 have? What about p^a for other natural numbers a?
6. Suppose we have numbers m, a, b, and when we apply division with remainder to m with a and m with b, we get $m = qa + r$ and $m = pb + s$. If $r \neq s$, prove that $a \neq b$. Is the converse true - i.e., if $r = s$, must we have $a = b$?
7. Does there exist a (nonzero) natural number x such that $x^2 = x + x$? For what numbers a can we find a nonzero natural number x that has the property $x^2 = ax$?