Math 189H Joy of Numbers Activity Log

Thursday, August 25, 2011

Pliny the Elder: "Why do we believe that in all matters the odd numbers are more powerful?"

Marston Bates: "Research is the process of going up alleys to see if they are blind."

We started with a short discussion about the current largest known prime. Numbers of the form $M_n = 2^n - 1$ are known as *Mersenne numbers* after Marin Mersenne (1588-1648), who first investigated their primality. A *Mersenne prime* is a Mersenne number which is prime. To date, only 47 are known, incuding the 9 (!) largest known prime numbers. These are the largest primes known mostly because there is a (fast) test, due to Lucas and Lehmer, to determine primality of Mersenne numbers, which essentially only works for Mersenne numbers, and is far faster than any other test so far discovered (for any kind of number).

We also discussed (what your instructor could not remember were called) *Sierpinski numbers*: these are numbers N so that for <u>every</u> choice of n the number $N \cdot 2^n + 1$ is <u>not</u> prime. John Selfridge proved that $N = 78557$ is Sierpinski; that is, that $78557 \cdot 2^n + 1$ is never prime. It was later conjectured that 78557 is the <u>smallest</u> Sierpinski number, an assertion which remains unproved. The SOB (= 'Seventeen or Bust') project was initiated to prove this conjecture, by finding , for the (at the time) 17 outstanding values of N less than 78557, values of n so that $N \cdot 2^n + 1$ is prime. Their work can be found at http://www.seventeenorbust.com/ ; there are still 6 values of N yet to verify. They are 10223, 21181, 22699, 24737, 55459, and 67607.

Then we turned our attention to our questions from last time. Several suggestions were offered for how to describe even/odd numbers:

n is even if it is divisble by 2.
n is even if it ends in 0,2,4,6, or 8 (the working man's definition!).
n is even if n things can be paired up one with another.
n is odd if it isn't even!
n is odd if pairing n things up leaves one left over.
n is odd if $n = 2x + 1$ for some other number x.
n is odd if it ends in 1,3,5,7, or 9.

The fourth suggestion prompted us to note that we had not yet described what <u>kinds</u> of numbers we were talking about! For the most part our explorations will center on the <u>natural</u> <u>numbers</u> $\mathbb{N} = \{1, 2, 3, 4 \ldots\}$ and the <u>integers</u> $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$. [The letter $\mathbb{Z}$ comes from the German word for number, 'Zahl'.]

For the purposes of demonstrating the answers to our motivating questions, we settled on the definitions:

An integer $n \in \mathbb{Z}$ is even if $n = 2x$ for some other integer $x \in \mathbb{Z}$.

[Notation: $\in$ means 'in' or 'is an element of'.]

An integer $n \in \mathbb{Z}$ is odd if $n = 2x + 1$ for some other integer $x \in \mathbb{Z}$.

With these, we could demonstrate the answers to our questions:

The sum of two even numbers is even, since if n and W are even, then $n = 2x$ and $W = 2F$ for some integers x and F, and then

$$n + W = 2x + 2F = 2(x + F)$$

so $n + W$ is also a multiple of 2. And the product of two odd numbers is odd, because if q and v are odd, then $q = 2r + 1$ and $v = 2d + 1$ for some $r, d \in \mathbb{Z}$, and then (FOIL!)

$$\begin{aligned} qv = (2r+1)(2d+1) &= (2r)(2d) + (2r)(1) + (1)(2d) + (1)(1) \\ &= 2(r2d) + 2(r) + 2(d) + 1 = 2(r2d + r + d) + 1 \end{aligned}$$

so qv is also 1 plus a multiple of 2. Our other assertions can be settled by similar calculations. Of course, in both of these demonstrations, we were employing properties of the integers, and in particular, properties of addition and subtraction, that we were already used to using. We made a list of them:

$a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ [distributivity]
$a(bc) = (ab)c$ and $a + (b + c) = (a + b) + c$ [associativity]
$ab = ba$ and $a + b = b + a$ [commutativity]

and after a little while we remembered that there are certain 'special' integers:

$a + 0 = a$ and $a \cdot 1 = a$ [adding 0 and multiplying by 1 do nothing!]

We then turned our attention to producing a formal description of what it means for an integer to be 'prime'; we ran out of time before completely settling this. We got as far as 'a number n is prime if it cannot be factored', which required us to figure out what a 'factor' of an integer was, which led us to the notion of one number 'dividing' another ('evenly'!):

$a \in \mathbb{Z}$ divides $b \in \mathbb{Z}$ [notation: $a|b$] if $b = aq$ for some other integer $q \in \mathbb{Z}$.

Equivalent ways to say the same thing include 'a is a factor of b' and 'b is a multiple of a'. From this idea, we ought to be able to build a workable definition of 'prime'.

[Using this new notation, it is possbile to state the Lucas-Lehmer test for primality of a Mersenne number $M_n = 2^n - 1$:

If we set $F_0 = 4$ and then continue to square the number and subtract 2, so $F_{k+1} = F_k^2 - 2$ (i.e., we keep taking the output of the function $F(x) = x^2 - 2$ and use it as the input again), then M_n is prime <u>precisely</u> <u>when</u> $M_n|F_{n-2}$.]

To stimulate discussion for Tuesday, we finished with the following questions:

If $a|b$ and $a|c$, what can we say, in terms of divisibility, about $a + b$? About ab?

If $a|(b + c)$, what can we say, in terms of divisibility, about b? About c?

If $a|(bc)$, what can we say, in terms of divisibility, about b? About c?