Math 189H Joy of Numbers Activity Log

Tuesday, September 6, 2011

David Hilbert: "The art of doing mathematics consists in finding that special case which contains all the germs of generality."

Pablo Picasso: "Computers are useless. They can only give you answers."

Every integer $N > 77$ can be written as a sum of integers $N = a_1 + a_2 + \cdots + a_n$ so that their reciprocals sum to 1, i.e., $\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = 1$.

Class began with a discussion of what was meant by one of the parts of the last problem on the exam: for which values of n is n^2+6n+5 a prime? Using $n^2+n-2 = (n+2)(n-1)$ as a model, the factorization of the polynomial tells us that most values of n yield composite numbers, unless (possibly) $n+2 = \pm 1$ or $n-1 = \pm 1$. This led us to wonder whether or not we allow negative numbers to be considered prime; our consensus was "yes" (?). But we're willing to be flexible on that!

Referring back to the instructor's 'favorite' prime, $428551 \cdot 2^{2006520}+1$ (which, as it happens has fallen to 99th on the list of largest primes, a new, 771,356 digit, prime, $75 * 2^{2562382} - 1$, was recently found), we noted that the method we have devised so far for testing for primes, trial division by all of the primes up to $\sqrt{N}$, would be terribly ineffective on such a number. It sounds very efficient: using 2,3,5, and 7 (the primes up to 10), trial division will yield a list of all primes up to $100 = 10^2$. That list can be used to build a list of the primes up to $10,000 = 10^4$, which generates a list of primes up to 10^8, and so on, and so on. But even on 'everyday' numbers N, of 100 to 200 digits, you would need to (a) have a list of primes up to half the number of digits of N, and (b) trial divide by all of them to test for primality. A basic rule of thumb is that the number of primes up to N is roughly $N/4\cdot$[the number of digits in N]. (Why? We may discuss this later!) So to find a 100-digit prime, we would need to use the primes less than 10^{50}, of which there are something more than 10^{47}. If we assume we can do a billion (10^9) trial divisions each second, then since there are around 10^6 seconds in a day and 10^3 (!) days in a year, we would finish testing a random 100-digit number (with a 1 in 400 chance of it being prime!) in roughly 10^{29} years. Which is an awfully long time to wait...

What we need is something different! Ideally, we would like some quick computation which would unerringly tell us if a number N were prime or not. Or if what we want is lots of primes, we'd like a little black box which keeps spitting out primes on demand. This could, for example, be a "prime-generating function", a function which every time I feed it new input, outputs another prime. There are, in fact, such functions (sort of): the following function (with 26 variables!) was found in 1976. Every positive number it spits out is prime (and it will spit out all primes):

$$N = (k+2) \cdot \big\{1 - \Big([wz+h+j-q]^2 + [(gk+2g+k+1)(h+j)+h-z]^2$$
$$+[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 + [2n+p+q+z-e]^2 - [e^3(e+2)(a+1)^2+1-o^2]^2$$
$$+[(a^2-1)y^2+1-x^2]^2 + [16r^2y^4(a^2-1)+1-u^2]^2 + [n+l+v-y]^2$$
$$+[(a^2-1)l^2+1-m2]^2 + [ai+k+1-l-i]^2$$
$$+[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2$$
$$+[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2$$
$$+[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 + [z+pl(a-p)+t(2ap-p^2-1)-pm]^2\Big)\big\}$$

is, if positive, always prime. [Negative numbers coming out of this formula could be anything, prime or composite.] (As was pointed out, this formula extends over a quarter of a page... Hm, does it?) This formula is fairly useless, though, since we don't know what input will produce a positive output! And if you look carefully, you'll note that most of the formula is 1 minus a bunch of squares, which is rarely positive! And from that, you can in fact notice that the prime it will spit out is $k+2$, so the only input that will ever spit out a prime requires k to be 2 less than a prime...

In the end, we aren't going to look for a 'quick' way to determine whether or not a number N is prime. Instead, we are going to settle for being occasionally wrong! What we would like to do is, essentially, look for our car keys under the street lamp instead of where we lost them, as the old joke goes, because they would be easier to find there. That is, we would like to increase the odds of finding a prime number, by learning where they are more likely to hide. There is this wonderful construction, due to Stan Ulam (who is known for, among other things, working on the Manhattan Project during WWII), which illustrates this point, known as the Ulam spiral. The story goes that Ulam was attending a lecture, and having gotten bored, started doodling. He wrote out the positive integers, starting with 1, as a 'spriral', travelling around in a couterclockwise direction filling out a square grid [refer to your handouts here]. He then marked which numbers were prime. What he saw before him exhibited much more 'structure' than he had expected; as we saw, the primes appear to populate certain diagonal lines more than others. [There is a conjectured explanation for this; we may discuss this later!] If we could predict which diagonals are more popular, for example, we could increase our chances of finding primes by looking only on those diagonals.

It is this kind of hidden structure that we would like to find; it tells us that there may be certain numbers that are more profitable (in both the mathematical (find primes!) and economical (sell primes!) sense) to look at than others. What we ultimately want (and will ultimately find!) is a quick way to look at a number and say 'No, not prime', so that we can spend our energies dealing with numbers that stand a better than average chance of being prime, instead of wasting (what was it?) 10^{29} years worth of computation on a number that has only a 1 in 400 chance of being prime, anyway. To carry the analogy too far, what we are postulating is that there is a 'secret' street lamp that primes hang out under; finding primes more easily amounts to figuring out what this street lamnp looks like!

Ultimately, this question comes down to: what makes a prime number different from a composite number anyway?. And is there a way to detect this difference, without finding a factor for the composite number? In the end, the difference between primes and composites is in how many numbers divide them; a prime p is divisible by by exactly 4 numbers (± 1 and $\pm p$), while a composite number has more divisors (as we will come to call them). What we would like, really, is a way to say 'You must have more divisors than a prime should, so you can't be prime', without actually finding the divisors!

We ended the class with a discussion of one of the thinking problems from a week ago: what numbers can you write as $5a + 7b$ for $a, b \in \mathbb{Z}$? We started generating a list, but after discovering that we had skipped some (possible partly because different people were playing by different rules: should a and b be positive? non-negative?), we tried to be a bit more systematic, writing out a grid with 0 in a corner and the multiples of 5 along the top, then creating new rows by successively adding 7 to the previous row. Once we did that, with a little searching we found that every number greater than (what was it?) 23 seemed like it would appear. All, in the end, that we needed was for a sequence of five consecutive numbers to appear; then we could add 5 to all of them to get the next five, and repeat that process forever. The question we didn't quite get to (which I am typing here in order to remind myself!) is, what happens if we instead repeatedly subtract 5?