Math 189H Joy of Numbers Activity Log

Thursday, September 1, 2011

George Will: "The nice part about being a pessimist is that you are constantly being either proven right or pleasantly surprised."

Bernd Matthias: "If you see a formula in the Physical Review that extends over a quarter of a page, forget it. It's wrong. Nature isn't that complicated."

$$153 = 1^3 + 5^5 + 3^3$$

We picked up our exploration of how we generated our list of the smallest primes with the observation from last time: factors of a number come in pairs. If $a|n$, then $bn = aq$ and so $q|n$ and we have found another factor. This can be used to cut the work of testing a number for primality even further. Using $n = 229$ as our model, this means that, for example, since $114 < 229/2 < 115$, any number between 115 and 228 has no chance of being a factor of 229, since there is nothing to pair it with; 1 is too small, and 2 is too big.

To be precise, since $2 \cdot 114 < 229 < 2 \cdot 115$, any number a between 115 and 228 will have $229 < 230 = 2 \cdot 115 \leq 2a$ and $a \leq 228 < 229$, so a is too small to be 229 and $2a$ is too large to be 229, so a cannot be a factor of 229.

But we can use the same idea to eliminate more potential factors of 229, knowing that we need need bother checking them. Since $76 < 229/3 < 77$ (or if division makes you nervous - we often leave the comfortable world of integers! - snce $3 \cdot 76 < 229 < 3 \cdot 77$), no integer between 77 and 114 can be a factor of 229, since for $77 \leq a \leq 144$ we have $229 < 231 = 3 \cdot 77 \leq 3 \cdot a$, and $2 \cdot a \leq 2 \cdot 114 = 228 < 229$, so $2a$ is too small to be 229 and $3a$ is too large.

Putting this together, since $2 \not| 229$ and $3 \not| 229$ [here we introduce for the first time the notation $a \not| b$, meaning 'a does not divide b'], no integer between 76 and 114, and no number between 115 and 228, can divide 229, either. Together this means that there is no need to check any integer between 76 and 228, simply because 2 and 3 do not divide 229. And we can keep going! Since $4 \not| 229$ and $229 < 4 \cdot 57$, now no integer between 57 and 228 divides 229. And since $5 \not| 229$ and $229 < 5 \cdot 46$, we can eliminate all $a \geq 46$. Four attempts at factors $(2, 3, 4, 5)$ have eliminated 4/5ths of the candidate factors between 2 and 229.

And eventually the range of numbers we needn't check (which keeps growing down from the right) will runinto the range of numbers we have checked (growing up from the right), and we run out of numbers to check! This happens when the last number we've checked, a, is bigger than $229/a$ (which is (below the) left end of the number we need't check). That is, we can stop when $229/a < a$, that is $a^2 > 229$. This happens when $a = 16$, since $16^2 = 256 > 229$ (but $15^2 = 225 < 229$. Since we can check that no integer less than 16 is a factor of 229, this means that 229 is prime!

This works in complete generality. Given a number N, to determine if N is prime, we can check, for each integer a with $2 \leq a \leq \sqrt{N}$, if $a|N$. If the answer is always 'No', then N is prime, since for every test which 'succeeds' (i.e., $a \not| N$; we've decided that being prime is good, so not being divisible by a number is a success!), the range of number that might divide N shrinks (from the right); if we reach the last integer below $\sqrt{N}$ having always succeeded, the boundary of the set of numbers we don't need to check has reached us, and nobody will be a factor. So N is prime!

This cuts the amount of work we need to do from around N trial divisions, from 2 to $N-1$, to around $\sqrt{N}$ trial divisions, from 2 to the last integer less than of equal to $\sqrt{N}$. And as we noted, still more can be done! If you have already tested for divisibilty by 2 qnd 3, there is no point in testing for divisibility by 4 or 6 (or 8 or 9 or...), since, e.g., if $9|N$ then since $3|9$ we would have discvoered that $3|N$.

This led us to the observation that *to test a number N to see if it is prime, it is enough to check to see if it is divisible by any of the prime numbers less than or equal to $\sqrt{N}$.* So, for example, since the only prime numbers up to 10 are 2, 3, 5, and 7, any number below 100 not divisible by one of these (and for 2, 3, and 5 we have quick tests!) must be prime. With this, and the 'trick' of simply starting at 7 and repeatedly adding 7 to identify the multiples of 7 as we went up the line (the ones to remember are the odd ones, 7,21,35,49,63,77,91), we could generate a complete list of all primes up to 100:

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97

There are, we found, 25 of them. With this list, we could bootstrap our way up, and test every number up to $10{,}000=(100)^2$ for primality. And then again, and again, and...!

We finished the class by firing up a little computer software, to demonstrate a point which will motivate much of what we will continue to do. The computer algebra system Maple 15 has two commands, 'isprime()' and 'ifactor()' [most CAS's have similar if not identical commands]. 'isprime' will return *'true'* or *'false'*; if false, then the number is definitely not prime, and if true, the number has a better than 99.99999999% chance of being prime. [Why the 'uncertainty'? That's one of the things we will talk about!] 'ifactor' will attempt to factor your integer N using a battery of procedures, starting with trial division by a list of 'small' primes [you can force this to be the only test with the command 'ifactor([number],easyfunc)'] and working its way through more sophisticated tests.

Typing in a randomly chosen semi-long number:

$$N = 871349852349752397856238562378652983563298653289456328568325629385629\\786378934786348976523875278234568236589326523987563298465832965983 4897$$

(having, as it happens, 139 digits), the command ifactor(N,easyfunc) found the 'small' prime factors

907 and 17970301, leaving

$$M = 534601192703857616209924601820181787314504767647872145297441409 7\\776177682941665717489771796397094782813220333767643969469676802 71$$

(with 129 digits) yet to factor. The program YAFU ("yet another factoring utility"") found the additional factor 7319702710991711519969669 (having 25 digits), but the remaining part of N

Th 1 September

$$\begin{multline*}Q = 73035916049031321504662941128228824459062815804321 3\\ 876558281228505123394188132498128969591496611129 44259\end{multline*}$$

(with 104 digits) is still not prime (according to ‘isprime’)! My computer(s) are still trying to factor Q.

The point is that there are programs which given a fairly large number like Q can in seconds decide that the number is composite, without knowing a proper factor of Q. And, in fact, it can take hours, days, weeks - even years - to actually find a factor. [A human being would be correspondingly slower on both tasks.]

How is that possible? How is it possible to (‘quickly’) know that a number is composite, without having the least clue what a factor of the number is? Tracking down an answer to this question will take us in some very interesting directions...