Prime Numbers

This is how you work out what prime numbers are. First you write down all the positive whole numbers in the world. Then you take away all the numbers that are multiples of 2. Then you take away all the numbers that are multiples of 3. Then you take away all the numbers that are multiples of 4 and 5 and 6 and so on. The numbers that are left are the prime numbers.

The rule for working out prime numbers is really simple, but no one has ever worked out a simple formula for telling you whether a very big number is a prime number or what the next one will be. If a number is really really big it can take a computer years to work out whether it is a prime number.

Prime numbers are useful for writing codes and in America they are classed as Military Material and if you find one over 100 digits long you have to tell the CIA and they buy it off you for $10,000. But it would not be a very good way of making a living.

Prime numbers are what is left when you have taken all the patterns away. I think prime numbers are like life. They are very logical but you could never work out all the rules, even if you spent all your time thinking about them.

From *The Curious Incident of the Dog in the Night Time*

We know a lot about primes. We know (as of 2008) a prime that is 12,978,189 digits long. You can read a list of the first fifty million primes[1]. But for each question we can answer, there's a similar one which has resisted the efforts of mathematicians for hundreds of years. To give you a taste, here is a list of some of the best theorems and open questions in prime numbers.

Great Theorems about Prime Numbers

(1) **There are infinitely many primes**
This was first proved by Euclid sometime around 350 BC. His proof was the same one that we did in class.

(2) **The Prime Number Theorem:**
Pick any really big integer N. The percentage of numbers less than N which are prime is approximately equal to $\frac{1}{\#N}$ where $\#N$ is the number of digits N has[2]. This was first proved in 1896.

(3) **Bertrand's Postulate:**
Pick any integer n that is larger than 1. There will always be a prime number that is greater than n but less than $2n$. This was proved in 1850.

[1] It's here: http://primes.utm.edu/lists/small/millions/

[2] More precisely, this approximation is given using the *natural logarithm* function, $\frac{1}{\ln(N)}$. The larger N is, the more accurate an approximation you get

Great Unanswered Questions about Prime Numbers

(1) **The Twin Primes Conjecture**
Are there infinitely many *twin* primes?

(2) **Mersenne primes**
Are there infinitely many primes of the form $2^p + 1$?

(3) **Goldbach's conjecture**
Can every even integer greater than two be written as the sum of two primes?

(4) **...and why not also**
Can every even integer greater than two be written as the *difference* of two primes?

(5) **Legendre's conjecture**
Take any number n. Will there always be a prime number greater than n^2 but less than $(n+1)^2$? [compare this to Bertrand's postulate, at the end of the 'solved' list]

Why do we continue to look for answers to these problems? Why not give up, since they haven't been solved for hundreds of years? First, there is still hope: quite recently (in 1995), a famous 350 year old unsolved problem from number theory was finally resolved. This is "Fermat's last theorem," proved by Andrew Wiles. Secondly – and this is especially important – finding the final answer to a famous unsolved problem is not always the point. In the words of number theorist Tom Apostol,

> *Repeated failure by eminent mathematicians to settle these problems by known procedures stimulates the invention of new methods, approaches, and ideas that, in time, become part of the mainstream of mathematics, and even change the way mathematicians think about their subject. This is certainly true of the prime number theorem: Early attempts to prove it stimulated the development of the theory of functions of a complex variable – a branch of mathematics that is the lifeblood of mathematical analysis. And efforts to prove Fermat's last theorem led to the development of algebraic number theory—one of the most active areas of modern mathematical research, with ramifications far beyond the Fermat equation.*

Exercises

(1) What algorithm is described at the beginning of the quote from *The Curious Incident* at the beginning of this reading?

(2) Show that Bertrand's postulate is not enough to prove Legendre's conjecture. That is, give an example of a number n so that $(n+1)^2$ is *less* than twice as big as n^2. Is this true for all really big numbers n?

(3) Pick an even integer between 100 and 200, and write it as the sum of two primes.