EMAT10001 Exercise Sheet 4.

Conor Houghton 2013-10-17

Exercise sheet

The difference between the work sheet and the exercise sheet is that the solutions to the exercise sheet won't be given and the problems are designed to be more suited to working on on your own, though you are free to discuss them in the work shop if you finish the work sheet problems. Selected problems from the exercise sheet will be requested as part of the continual assessment portfolio.

1. Determine the set of integers for which the number of divisors is odd. Make a general conjecture and prove your claim.
2. $n! = n(n-1)(n-2)\ldots 2\cdot 1$ so $5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120$. What are the prime factors of 12!.
3. If a and b are integers does $a^2|b^3$ imply $a|b$? Prove or disprove.
4. Show $2|(n^2-n)$.
5. Show the numbers $6k+5$ and $7k+6$ are co-prime for every $k \geq 1$.
6. Write a program to implement the Euclid algorithm.
7. Extend your Euclid algorithm so that it returns $(a,b) = ma + nb$.
8. Write a program to calculate primes using the Sieve of Eratosthenes.
9. Write a program to find the Euler Totient of numbers of modest size.
10. Imagine you wanted to calculate $a^b \bmod c$ for large values of a and b. The straightforward approach of calculating a^b and then taking its mod is inefficient and will overwhelm data types like `int`. The usual approach is to write b in the binary form

$$b = b_0 + 2b_1 + 4b_2 + 8b_3 + \ldots \tag{1}$$

with all the b_is one or zero. Now $a^2 \bmod c$ is easy to work out by squaring and modding, squaring that $(a^2)^2 \bmod c$ gives a^4 and so on. Use this to write a program to work out $a^b \bmod c$ which will work provided a^2 fits into `int`.

Challenge

There are copies of *What is the name of this book?* and a kitkat available to the first person to solve each of the projecteuler.net problems 3, 50, 69 and 214; that is, there are four prizes, one for each problem. Provide proof by sending a screen shot of the congratulations page, I will announce on the website when each of the problems is solved.