EMAT10001 Exercise Sheet 5.

Conor Houghton 2013-10-17

Introduction

There is the usual bounty for errors and typos, 20p to £2 depending on how serious it is.

Some of these questions are taken from *Number Theory with Computer Applications* by Ramanujachary Kumanduri and Cristina Romero.

Useful facts

- $a \equiv b \pmod{m}$ iff $m|(a-b)$.
- $(a, m) = 1$ if and only if there exists an a^{-1} such that $aa^{-1} \equiv 1 \pmod{m}$. This can be found using the Euclid algorithm.
- The Euclid algorithm is: set $x = a$ and $y = b$ where $a > b$, then, while $y! = 0$ set $r = x \bmod y$ and then let $x = y$ and $y = r$. If $y = 0$ the answer is x.

Some common mathematical notation

- **Z** or $\mathbb{Z}$, the integers, that is, whole numbers like zero, 67 and -120.
- **N** or $\mathbb{N}$, the natural numbers are a subset of the integers. Unfortunately there is no universal agreement on whether they are the non-negative integers: $\{0, 1, 2, 3, \ldots\}$ or the positive integers: $\{1, 2, 3, \ldots\}$.
- **Q** or $\mathbb{Q}$, the rational numbers; there are numbers of the form a/b where a and $b \neq 0$ are integers.
- **R** or $\mathbb{R}$, the real numbers; these are the numbers used to measure continuous quantities.
- $\forall$ for all, as in $x^2 \geq 0 \; \forall x \in \mathbf{Z}$.
- $\exists$ exists, as in $\forall x \in \mathbf{N} \; \exists p \in \mathbf{N}$ with $p > x$ and p a prime.
- iff: if and only if.

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. What is the inverse of 606 modulo 77? What is the inverse of 77 modulo 606?
2. Is 1111 congruent to 11 modulo 111?
3. Solve $42x \equiv 90 \pmod{156}$.
4. For the numbers from twenty to thirty say which are congruent to five modulo 13 and which are conguent to 13 modulo five.
5. Show that if n is odd then $n^2 \equiv 1 \pmod{8}$.
6. Let p be an odd prime. Find the values of x so that it is its own inverse modulo p.
7. Write a short program that allows you to input three numbers, a, b and c of modest size and tells you if $a \equiv b \pmod{c}$.
8. Write a program that tests if a has an inverse modulo m and which finds it if it does.
9. Write a program that automatically attempts to decode a passage encryped using the Caesar cipher by assuming the most letter is 'e'.

Challenge

There is either a kitkat and copy of *What is . . .* or a box of chocolates, your choice, for the first person to solve `projecteuler.net` problem 59. Provide proof by sending a screen shot of the congratulations page, I will announce on the website when the problem is solved. There is also a grand prize of a blown, that is empty, ostrich egg for the first person to solve 25 `projecteuler.net` problems, prove it with a screen shot of the progress page.