COMS10003 Workshop Sheet 8.

Julian Gough 2014-11-20

Introduction

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.

Work sheet

1. Use the Euclid algorithm to find x and y, integers, so that $9 = 945x + 2421y$.
2. Prove that congruence is an equivalence relation. That is show
   (a) Reflexivity: $x \equiv x \pmod{m}$.

(b) Symmetry: if $x \equiv y \pmod{m}$ then $y \equiv x \pmod{m}$.

(c) Transitivity: if $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$ then $x \equiv z \pmod{m}$.

This is not a hard question, the proofs are only a line or so long.

3. Consider the set of all well-defined functions $f(x)$ where x is a real number. Now define $f(x) \sim g(x)$ if $f(0) = g(0)$. Prove this is an equivalence relation.

4. Prove the individual properties of congruences. If a, b, c, d are integers and m a positive integer then

   (a) $a \equiv b \pmod{m}$ implies $ac \equiv bc \pmod{m}$.

   (b) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $a + c \equiv b + d \pmod{m}$.

   (c) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $ac \equiv bd \pmod{m}$.

   (d) $a \equiv b \pmod{m}$ implies $a^k \equiv b^k \pmod{m}$ for positive integers k.

   (e) $a \equiv b \pmod{m}$ and $d|m$ for some d a positive integer then $a \equiv b \pmod{d}$.

   (f) $ac \equiv bc \pmod{m}$ implies $a \equiv b \pmod{m/(c,m)}$.

   The last one is harder than the rest, start by letting $d = (c, m)$ and noting that this means $c = c'd$ and $m = m'd$.

5. Is -2 congruent to 31 modulo 11?

6. Is 77 congruent to 5 modulo 12?

7. Find the inverse of 67 modulo 119 and the inverse of 119 modulo 67.

8. By looking at all the possibilities, show that 12 has no inverse modulo 18.

9. Solve $11x \equiv 28 \pmod{37}$.

10. Consider $(p-1)! = (p-1) \cdot (p-2) \ldots 1$ where p is an odd prime. Now modulo p only one and $p - 1 \equiv -1 \pmod{p}$ are their own inverse; every other element has a unique inverse different from itself. Now by pairing each element with its inverse show that $(p-1)! \equiv -1 \pmod{p}$. This is known as Wilson's Theorem.

    The next few problems are about cryptography, this is in preparation for next week when we will look at RSA. The cryptographic schemes here are simpler and don't really rely on the number theory we have been doing.

11. The key idea behind cryptography is to keep messages secret. One of the most widely know cryptography techniques is called Caesar's cipher. The idea behind this is to shift all the letters a fixed amount down the alphabet. See if you can work out how this works and decipher these texts, each has a different shift.

    (a) Aqwtg iqppc pggf c dkiigt dqcv

(b) Vlr hklt elt ql tefpqib, alkq vlr, Pqbsb? Vlr grpq mrq vlro ifmp qldbqebo xka yilt.

(c) Rpyewpxpy, jzf nlye qtrse ty spcp. Estd td esp Hlc Czzx.

12. One problem with Caesar's cipher is that you can just try every shift until you find one that makes sense. There are ways to make this harder, but many schemes are vulnerable to frequency analysis, for example, for Caesar's cipher, if you have lots of text you can just guess the most common letter is coding 'e' and use that to calculate the shift and more complicated versions of this apply to more complicated ciphers. Vigenère's cipher is designed to combat this. In this cipher you do modular arithmetic on letters, so for simplicity ignore the space and punctuation and number the letters zero through to 25. Now, to add two letters add the corresponding numbers modulo 26. Hence a+b=b, b+b=c and c+c=e. Now to use Vigenère's cipher choose a code key, say 'casablanca' and to encode 'tomorrowisanotherday' you add c to t, a to o, s to m, a to o, b to r, l to r, a to o, n to w, c to i and a to s. At this points you have run out of letters in casablanca, so you start again, c to a, a to n and so on. Work out the Vigenère cipher of 'tomorrowisanotherday' using 'casablanca' and the cipher of 'bondjamesbond' using 'drno'.

13. Decode 'ihczsfmkoyysexgpwkqwmumiwrvlqeqa' with the key 'maewest'.

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.

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 congruent 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 encrypted using the Caesar cipher by assuming the most letter is 'e'.

Challenge

See if you can solve `projecteuler.net` problem 59. see if you can be the first to post on the unit forum a screen shot of the congratulations page for each one.