EMAT10001 Workshop Sheet 4.

Conor Houghton 2013-10-17

Introduction

This worksheet is about modular arithmetic, primes, greatest common divisors, the Euler totient function and equivalence relations.

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

- $r = a \bmod c$ means $a = mb + r$ and $0 \leq r < b$.
- A prime number is one that has exactly two divisors.
- Two numbers are co-prime, also called relatively prime, if $(a, b) = 1$.
- 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.
- The *Euler Totient function*:

$$\phi(a) = |\{b \leq a | (a, b) = 1\}| \tag{1}$$

  so $\phi(a)$ is the number of numbers less or equal a and co-prime with it. So, for example, $\phi(6) = 2$ because only one and five are less than six and co-prime with it.

Euclid algorithm, worked example

I got the timing of my lecture a bit wrong and I never did an example of the Euclid algorithm, so here is one. We want to find $(972, 3834)$. Hence, set $x = 3834$ and $y = 972$. Now

$$3834 = 3 * 972 + 918 \tag{2}$$

so now $x = 972$ and $y = 918$ and we get

$$972 = 918 + 54 \tag{3}$$

then with $x = 918$ and $y = 54$

$$918 = 17 * 54 \tag{4}$$

so in the next round y would be equal zero so $(972, 3834) = 54$. We can also go backwards.

$$54 = 972 - 918 \tag{5}$$

and $918 = 3834 - 3 * 972$ so

$$54 = 972 - (3834 - 3 * 972) = 4 * 972 - 3834 \tag{6}$$

which express $54 = (972, 3834)$ in the form $972n + 3834m$.

Work sheet

1. Think of two numbers a and $b < a$, now calculate $r = a \bmod b$. Do this five times with bigger and bigger a.

2. Prove that
$$(a + b \bmod c) = [(a \bmod c) + (b \bmod c) \bmod c] \tag{7}$$
and
$$(ab \bmod c) = [(a \bmod c)(b \bmod c) \bmod c] \tag{8}$$

3. What number less than 100 has the most divisors?

4. If p is a prime number how many divisors of p^n are there?

5. If a, b, c, x and y are positive integers prove

   (a) If $a|b$ and $x|y$ then $ax|by$.

   (b) If $a|b$ and $b|c$ then $a|c$.

   (c) If $a|b$ and $b \neq 0$ then $a < b$.

   (d) If $a|b$ and $a|c$ then $a|(bx + cy)$.

6. Why isn't one a prime?

7. The next few questions are about the Euler totient function, which is defined in the useful facts section. First, think of a two digit number a and work out $\phi(a)$. Do this five times.

8. If p is prime what values of $a \leq p^n$ have $(a, p^n) > 1$?

9. If p is prime, what is $\phi(p)$?

10. If p is prime, what is $\phi(p^r)$?

11. If $(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$; you can look this up, it is a consequence of the Chinese Remainder Theorem, which we aren't covering. Now, given the prime factorization of n is
$$n = \prod p_i^{r_i} \tag{9}$$
what is $\phi(n)$? Note that this means working out $\phi(n)$ is easy if you can factorize n, for large numbers this is a big if! Use your formula for some of the values of $\phi(n)$ you calculated above.

12. Prove $(a, b) = (a - b, b)$.

13. This question is about drawing a star without lifting your pencil off the paper. Imagine there are n points equidistant around a circle. You want to draw a star by not lifting your pencil off the paper, it doesn't count as a star if you go from one point to the next, also, stars are symmetric, the angle at each of the points must be the same. So, for example, the star of David doesn't count because it involves two disconnected paths, but for $n = 5$ there is one and $n = 7$ there are two. How many different starts are there for n points?

14. Think of two three digit numbers a and b. Work out their greatest common divisor by first factorizing them. Repeat the calculation using the Euclid algorithm. Express the greatest common divisor in the form $ma + nb$ for integers a and b. Do this five times.

15. Prove that the slowest convergence for the Euclid algorithm occurs when the two numbers are consecutive terms in the Fibonacci sequence.

16. Prove congruence is an equivalence relation.

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

$$b = b_0 + 2b_1 + 4b_2 + 8b_3 + \ldots \tag{10}$$

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.