MA7010 – Number Theory for Cryptography

Assignment 1 – Primes and Prime Testing

The questions on page 2 need to be completed and uploaded to Weblearn no later than 3.00pm on Friday 12th January.

While you can talk about the assignment to other students on the module the final submission must be your own work and the University’s policy on plagiarism and assessment offences will be applied if necessary. You may make use of the fragments of Maple code and procedures that have been developed in the workshops but will need to add to these with some additional code.

You can attempt the assignment in Python or any other programming language if you prefer.

25% of the marks are reserved for your written explanations of your results which should form part of the same document as your results. The majority of these marks are assigned to the final question but you should also annotate and explain your answers to all the questions so that your results are easily understandable. 10% of the marks are allocated for the elegance and efficiency of your solutions. 65% of the marks are allocated to answering Questions 1-5 as per the breakdown overleaf.

Each student will be allocated a different range of numbers so your answers should be unique. The number ranges are:

|  |  |  |
| --- | --- | --- |
| Name | Lower Range | Upper Range |
| Navjeet | 1700 | 2000 |
| Stuart | 2300 | 2600 |
| Ajeesh | 2800 | 3100 |

The questions will ask you about numbers in a range; you should give answers for all values between your lower and upper ranges inclusive.

Question 1 (15 marks):

For the number range assigned to you answer the following using only basic sieving algorithms for a) and the commands ifactors and ifactor, ops, nops for b):

1. List the elements of the set A = {all primes p in the range}, B = {all composite numbers in the range}
2. List the elements of the set C where C = {composite numbers n = pq in your range which are the product of exactly two distinct primes p and q}.
3. Choose any three element of the set B and then randomly select 5 values of a for each element. Apply the gcd test for each of the 12 cases and report on how accurate it is in determining that a number is composite.

Question 2 (10 marks):

Find all Carmichael Numbers in your range using:

1. A direct method employing the Fermat Test that shows that a composite number n has no Fermat Witnesses;
2. Checking which numbers satisfy Korselt’s Criteria.

Question 3 (25 marks):

Take the first five elements n of the set B of composite numbers with 2 factors in your range (or all numbers if you find there are less than 10). The Miller Rabin test states that at most ¼ of numbers a that are randomly chosen will give the answer that n is ‘probably prime’. How close can you get to this maximum, (i.e. which of your 5 choices has the highest proportion of possible a’s that would fail the Miller Rabin test).

What composite numbers m between 50 and 100 have the highest proportion of Miller Rabin failures? (For each number in the range work out the proportion of a’s that produce the answer ‘m is probably prime’). Look at the prime factorisation of these numbers and see if it suggests any patterns about which numbers are vulnerable to giving false answers in Miller Rabin.

Question 4 (15 marks):

1. Choose any three elements of your set A and calculate the value of r used in the AKS primality test;
2. Write a single procedure that implements the AKS test using the code that we have seen;
3. Take the elements of the set B in turn and decide how many fail the test at each of steps 1, 2, 3, 4, 5.

Question 6 (contributes to the ‘written explanation’ category worth 25% of the marks, you should write 400-500 words summarising your conclusions):

Consider the tests we have seen so far in the module

i) a Fermat Test calculating am-1 mod m

ii) a gcd test on a and m

iii) a Miller Rabin test

iv) Trial division/sieving methods

v) The AKS primality test

Thinking about factors such as:

* the probability that the test produces a clear answer,
* the amount of work that it involves

summarise which test you would recommend for deciding if a number is prime or not.

Does the size of the target number affect your answer? Does it change for:

1. Numbers less than 10 000 000
2. Numbers bigger than 1 000 000 000 000
3. Numbers bigger than 10^100