Michaelmas Term 2012 J. M. E. Hyland

Number Theory: Example Sheet 4

I have not felt able to identify exactly 12 questions for the supervisions. I have simply adapted the sheet produced by Vicky Neale last year without the further questions of previous sheets. There is one question on the other side of the sheet!

1. Find two solutions in positive integers x and y of the equation $x^2 - dy^2 = 1$ when $d = 3$, 7, 13, 19, 46.

2. Let n and m be positive integers such that n is not a square and such that $m \leqslant \sqrt{n}$. Prove that if x and y are positive integers satisfying $x^2 - ny^2 = m$ then x/y is a convergent of $\sqrt{n}$.

3. Determine which of the equations $x^2 - 31y^2 = 1$, $x^2 - 31y^2 = 4$ and $x^2 - 31y^2 = 5$ are soluble in positive integers x and y. For each that is soluble, exhibit at least one solution.

4. Assume that n is an integer greater than 1 such that $F_n = 2^{2^n} + 1$ is composite ($n = 5$, ...). Prove that F_n is a pseudoprime to the base 2.

5. Prove that there are 36 bases for which 91 is a pseudoprime. More generally, show that if p and $2p-1$ are both prime numbers, then $n = p(2p-1)$ is a pseudoprime for precisely half of all bases.

6. Let $n = (6t+1)(12t+1)(18t+1)$, where t is a positive integer such that $6t+1$, $12t+1$ and $18t+1$ are all prime numbers. Prove that n is a Carmichael number. Use this construction to find three Carmichael numbers.

7. Find the number of bases b for which 561 is an Euler pseudoprime. Show that there are precisely 10 bases for which 561 is a strong pseudoprime.

8. Let p be a prime greater than 5. Prove that $N = (4^p + 1)/5$ is a composite integer. Prove that N is a strong pseudoprime to the base 2.

9. Prove that if N has a factor which is within $\sqrt[4]{N}$ of $\sqrt{N}$, then Fermat factorisation must work on the first try.

10. Use Fermat factorisation to factorise the integers 8633, 809009, and 92296873.

11. Explain why when we use the continued fraction algorithm for factorising N, there is no need to include in the factor base B any prime with $\left(\frac{N}{p}\right) = -1$.

12. Let $N = 2701$. Use the B-numbers 52 and 53 for a suitable factor base B to factor 2701.

13. Use Pollard's $p-1$ method with $k = 840$ and $a = 2$ to try to factorise $N = 53467$. Then try with $a = 3$.

14. Use the continued fraction algorithm to factorise the integers 9509, 13561, 8777 and 14429.

Email any comments, suggestions and queries to `m.hyland@dpmms.cam.ac.uk`.