Number Theory: Example Sheet 4 of 4

Throughout this sheet, N denotes an odd positive integer.

- 1. Let d and m be positive integers such that d is not a square and such that $m \leq \sqrt{d}$. Prove that if x and y are positive integers satisfying $x^2 dy^2 = m$ then x/y is a convergent of \sqrt{d} .
- 2. 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.
- 3. Find two solutions in positive integers x and y of the equation $x^2 dy^2 = 1$ when d = 3, 7, 13, 19.
- 4. Find all bases for which 39 is an Euler pseudoprime.
- 5. Let N be an odd composite integer.
 - (i) Show that if N is a Carmichael number, then N is square-free.
 - (ii) Show that N is a Carmichael number if and only if N is square-free and p-1 divides N-1 for every prime p dividing N.
 - (iii) Show that if N is a Carmichael number, then N is the product of at least three distinct primes.
 - (iv) Find the smallest Carmichael number.
- 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. (You will need to come up with a better method than simply trying $t = 1, 2, 3, \ldots$)
- 7. 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.
- 8. Let N = 561. Find the number of bases b for which N is an Euler pseudoprime. Show that there are precisely 10 bases for which N is a strong pseudoprime.
- 9. 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.
- 10. 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.
- 11. 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.
- 12. Use Fermat factorisation to factor the integers 8633, 809009, and 92296873.

- 13. 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 p with $\left(\frac{N}{p}\right) = -1$.
- 14. Let N=2701. Use the *B*-numbers 52 and 53 for a suitable factor base *B* to factor 2701.
- 15. Use Pollard's p-1 method with k=840 and a=2 to try to factor N=53467. Then try with a=3.
- 16. Use the continued fraction algorithm to factor the integers 9509, 13561, 8777 and 14429.