Number Theory – Problem Sheet 4

1. Calculate $a_0, \dots, a_4$ in the continued fraction expansions of e and π.

2. Let a be an integer ≥ 1. Determine explicitly the real number whose continued fraction is $[a, a, a, \dots]$.

3. Determine the continued fraction expansions of

$$\sqrt{3}\ ,\ \sqrt{7}\ ,\ \sqrt{13}\ ,\ \sqrt{19}\ ,\ \sqrt{46}.$$

4. Let N and M be positive integers such that N is not a square and $M \leqslant \sqrt{N}$. If x, y are positive integers satisfying $x^2 - Ny^2 = M$, prove that x/y is a convergent of $\sqrt{N}$.

5. Determine which of the equations

$$x^2 - 31y^2 = 1,\quad x^2 - 31y^2 = 4,\quad x^2 - 31y^2 = 5$$

are soluble in positive integers x, y. If they are soluble, exhibit at least one solution.

6. Find two solutions in positive integers x, y of the equation

$$x^2 - Ny^2 = 1$$

when $N = 3, 7, 13, 19, 46$.

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

8. Use Fermat factorization to factor the integers
8633; 809009; 92296873.

9. In the continued fraction algorithm for factoring N, explain why there is no need to include in the factor base B any prime p with $\left(\frac{N}{p}\right) = -1$.

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

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

12. Use the continued fraction algorithm to factor the integers

9509; 13561; 8777; 14429.

(See Koblitz, p. 147-148).