

MTH6128

Number Theory

Assignment 5

For handing in on 17 February 2012

You should hand in your solution to the starred question only.

*Write your name and student number at the top of your assignment before handing it in. Staple all the pages together. Post the assignment in the **GREEN** post-box on the **GROUND floor** of the Maths building before 16:00 on Friday.*

1 (*) This question is from the 2010 exam paper.

- (a) State the Chinese Remainder Theorem.
- (b) Find the general solution of the simultaneous congruences

$$x \equiv 3 \pmod{7}, \quad x \equiv 1 \pmod{11}.$$

- (c) State and prove Fermat's Little Theorem.
- (d) Use Fermat's Little Theorem to prove that, for any integer n ,

$$n^{37} \equiv n \pmod{13} \quad \text{and} \quad n^{37} \equiv n \pmod{19}.$$

- (e) Deduce that, for any integer n ,

$$n^{37} \equiv n \pmod{741}.$$

2 (a) Calculate the values of the continued fractions $[\overline{1; 2, 3}]$ and $[4; \overline{1, 2, 3}]$.

- (b) Find the continued fraction for $3 + \sqrt{11}$.

3 In the lectures, we saw a proof using continued fractions of the following theorem:

Let α be an irrational real number. Then there are infinitely many rational numbers p/q such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

This exercise outlines an alternative proof. Fill in the details.

(a) Choose any positive integer n and consider the numbers $x_k = k\alpha - \lfloor k\alpha \rfloor$ for $k = 0, 1, 2, \dots, n$.

(b) Divide the unit interval $[0, 1)$ (closed on the left, open on the right) into n subintervals

$$[0, 1/n), [1/n, 2/n), \dots, [(n-1)/n, 1).$$

(c) The $n+1$ numbers x_0, x_1, \dots, x_n lie in these n intervals. Show that there must be two of them, say x_k and x_l , which belong to the same interval, with $k > l$ (say). Hence $|x_k - x_l| < 1/n$.

(d) Put $q = k - l$. Show that $q\alpha$ differs from the nearest integer (say p) by less than $1/n$.

(e) Deduce that

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{nq} < \frac{1}{q^2}.$$

(f) Given any such rational approximation p_i/q_i for α , show that we can choose n large enough that the rational approximation p_{i+1}/q_{i+1} produced by the above method is different from p_i/q_i . Specifically, if we choose n large enough that $n > |\alpha - p_i/q_i|^{-1}$, then

$$\left| \alpha - \frac{p_{i+1}}{q_{i+1}} \right| < \frac{1}{nq_{i+1}} < \frac{1}{n} < \left| \alpha - \frac{p_i}{q_i} \right|.$$

(g) Conclude that we get infinitely many such rational approximations.