

568 NUMBER THEORY II, SPRING TERM 2007, PROBLEMS 10

*Return by Tuesday 10th April*

1. Show that if  $\alpha_1, \dots, \alpha_n$  are real numbers and  $R \geq 2$  is an integer, then there are  $a_1, \dots, a_n$  and  $q$  with  $1 \leq q \leq R^n - 2^n + 1$  such that

$$|\alpha_1 - a_1/q| \leq q^{-1}R^{-1}, \dots, |\alpha_n - a_n/q| \leq q^{-1}R^{-1}.$$

The case  $n = 1$ ,  $R = Q + 1$  is Dirichlet's theorem.

2. Show that if  $\alpha_1, \dots, \alpha_n$  are real numbers and  $Q_1, \dots, Q_n$  are positive integers, then there are  $q_1, \dots, q_n$  not all zero and  $a$  with  $|q_1| \leq Q_1, \dots, |q_n| \leq Q_n$  such that

$$|\alpha_1 q_1 + \dots + \alpha_n q_n - a| \leq (Q_1 \dots Q_n + 1)^{-1}.$$

Note this conclusion is not very useful unless  $\alpha_1, \dots, \alpha_n, 1$  are linearly independent over  $\mathbb{Q}$ . In the contrary case it is trivial provided that the  $Q_j$  are large enough.

3. Let  $p$  denote a prime number with  $p \equiv 1 \pmod{4}$ . Then we know that there is an  $x$  with  $0 < x < p$  such that  $x^2 + 1 \equiv 0 \pmod{p}$ . By Dirichlet's Theorem, or otherwise, show that there are integers  $a, q$  with  $1 \leq q < \sqrt{p}$  such that  $s = xq - pa$  satisfies  $|s| < \sqrt{p}$ . Prove that  $s^2 + q^2 = p$ .

4. (R. Sherman Lehman, 1974.) Suppose that  $n$  has a divisor  $d$  with  $n^{\frac{1}{3}} < d \leq n^{\frac{1}{2}}$ . Show that there is a  $t$  with  $1 \leq t \leq n^{\frac{1}{3}} + 1$ ,  $y$  with  $4tn \leq y^2 \leq 4tn + n^{\frac{2}{3}}$  and an  $x$  so that  $4tn = y^2 - x^2$ . Deduce that this gives a simple method in  $O(n^{\frac{1}{3}})$  steps for finding non-trivial factors of composite numbers and of proving primality for prime numbers. This can be used as a basis for an algorithm which is both practical on small pocket calculators and appreciably faster than trial division.

Hint: Use Dirichlet's theorem to find  $a$  and  $q$  with  $x = |\frac{n}{d}q - ad|$  suitably small and put  $t = aq$ .