MA014G

Algebra and Discrete Mathematics A Assignment Block 3

To get the bonus points you must submit you solutions by 10am on Monday 1 October 2007.

Question 1

Carefully study Theorem B3.3 from the study guide for Block 3 and its proof which is given below. Then answer questions (a)-(e).

Theorem B3.3 Let m, n and d be integers such that d|m and d|n. Then d|(sm + tn) for all integers s and t.

Proof.

As m and n both are divisible by d, there exists two integer quotients q_1 and q_2 such that

$$m = dq_1$$
 and $n = dq_2$. (*)

Thus

$$sm+tn = s(dq_1) + t(dq_2) = d(sq_1+tq_2), \quad (**)$$
 and so $d|(sm+tn)$. \Box

- (a) What is meant by d|m, i.e. what is meant by saying that d divides m?
- (b) Which theorem or definition guarantees the existence of q_1 and q_2 satisfying (*)?
- (c) Explain carefully why the two =-signs hold in the computation (**).
- (d) Consider the computation (**). Explain why the term $sq_1 + tq_2$ is an integer.
- (e) Explain why the computation (**) proves that d|(sm+tn).

Question 2

Assume that $3|(2^{n-1}-1)$ for some integer $n \ge 1$. Prove that then $3|(2^{n+1}-1)$ also.

Question 3

- (a) Use Euclid's Algorithm to show that gcd(3571, 1753) = 1.
- (b) Find integers s and t with s > 0 and t < 0 such that 3571s + 1753t = 1.
- (c) Find integers k and ℓ with $\ell > 0$ and k < 0 such that $3571k + 1753\ell = 1$.

Question 4

The Fundamental Theorem of Arithmetic says that, apart from the order of the factors, there is a unique factorisation of 22374 into one unit and a finite number of positive primes. Showing all your working, find this factorisation of 22374 without using a calculator.