

13 October 2006

OWO Exercise Sheet      Linear Algebra I for MCS  
Winter Term 2006/2007

**(E0.1) [A simple proof.]**

Fill in the case of multiplication in the proof of Lemma 2.1 of the handout.

**(E0.2) [Modular Exponentiation.]**

Show some of the following claims (Exercise 1 in the handout):

- (i)  $3^{444} + 4^{333} = 0 \pmod{5}$
- (ii)  $2^{999} + 5^{999} = 0 \pmod{7}$       [similarly for all odd exponents]
- (iii)  $5^{222} - 2^{222} = 0 \pmod{7}$       [similarly for all even exponents]

Following the modular exponentiation procedure by hand, first compile tables of repeated squares mod  $n$ , then determine the relevant binary digits of the exponents.

**(E0.3) [Arithmetical reasoning.]**

Fill in the missing part in the combinatorial proof of Fermat's little theorem. Show that the smallest positive period of any circular colour pattern of length  $n$  must divide  $n$ .

A point for discussion: how would you formalise the notion of *colour pattern* and of *period* in order to make such arguments more formal?

**(E0.4) [Complexity of Euclid's algorithm.]**

Show that if  $a_0 > b_0 > 0$  are such that  $\text{EUCLID}(a_0, b_0)$  involves at least two further calls, first  $\text{EUCLID}(a_1, b_1)$  and then  $\text{EUCLID}(a_2, b_2)$  say, then  $a_2 < a_0/2$  and  $b_2 < b_0/2$ .  
(Cf. Exercise 2 in the handout)

**(E0.5) [Hand-cranking an RSA toy example.]**

Based on primes  $p = 7$  and  $q = 11$  and on  $e = 13$  for the public key, follow through the main steps of finding a matching secret key  $d$  and check an encryption/decryption example of your choice by hand. Also look at the instance of Little Fermat involved in checking correctness of the transformation pair.