

### Tutorial 4

1. Show that any non-zero homomorphism from a field  $F$  to a field  $E$  must be injective.
2. (Euclidean Algorithm) Let  $a_1, a_2 \in \mathbb{Z}$  with  $a_1 > a_2 \geq 0$  or  $a_1 = a_2 > 0$ , and whenever  $a_i \neq 0$  define  $a_{i+1}$  by the conditions

$$a_{i-1} = q_i a_i + a_{i+1}, \text{ and } 0 \leq a_{i+1} < a_i.$$

That is,  $a_{i+1}$  is the remainder when  $a_{i-1}$  is divided by  $a_i$ . Let  $k$  be the largest integer such that  $a_k \neq 0$  (so that  $a_1 \geq a_2 > \dots > a_{k+1} = 0$ ).

- (i) Calculate  $k$  and  $a_k$  in the case  $a_1 = 117$  and  $a_2 = 51$ .
  - (ii) Show that if  $e \in \mathbb{Z}$  satisfies  $e|a_1$  and  $e|a_2$  then  $e|a_i$  for all  $i$  from 1 to  $k$ .
  - (iii) Show that  $a_k$  is a divisor of all of  $a_{k-1}, a_{k-2}, \dots, a_2, a_1$ .
  - (iv) Deduce that  $a_k = \gcd(a_1, a_2)$ .
3. In this question assume  $a, b, c$  are integers.
    - (i) Show that if  $(a, b) = 1$  then  $a|c$  and  $b|c$  imply  $ab|c$ .
    - (ii) Show that if  $(a, b) = d$ , then  $(a/d, b/d) = 1$ .
    - (iii) An integer  $h > 0$  is called the lowest common multiple of integers  $a$  and  $b$  if  $a|h$  and  $b|h$  and if  $a|k$  and  $b|k$ , then  $k$  is a multiple of  $h$ .  
So if a lowest common multiple exist it is unique.  
Show that if  $a, b \in \mathbb{N}$  are not both zero then  $h = ab/(a, b)$  is the lowest common multiple of  $a$  and  $b$ .
  4.
    - (i) Show that  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ,  $x \mapsto (x \bmod 2, x \bmod 3)$  is a ring homomorphism and determine  $\ker \phi$ .
    - (ii) Use the first isomorphism theorem to deduce that

$$x \bmod 6 \mapsto (x \bmod 2, x \bmod 3)$$

defines a ring isomorphism from  $\mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .

5. (Chinese Remainder Theorem) Suppose  $m_1, m_2, \dots, m_n$  are pair-wise relatively prime integers, all greater than 1. Then any set of simultaneous congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \dots \quad x \equiv a_n \pmod{m_n},$$

has a solution, and it is uniquely determined  $\pmod{m_1 m_2 \dots m_n}$ .