Imperial College London

DEPARTMENT OF MATHEMATICS
IMPERIAL COLLEGE LONDON
Academic Year 2022-2023

Introduction to University Mathematics **MATH40001/MATH40009**

Part II – Problem Sheet 2

In the following questions, you may use results stated (but not proved) in lectures.

1. (a) ✦ Consider the sequence $\{a_n\}$ defined as $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$. Show that $a_n < 2^n$ for all n.
   (b) ✦ 2^n people are arranged in a circle and numbered from 1 to 2^n consecutively. Starting at person number 1, every second person is eliminated (i.e. person number 2, 4, 6,...) until only one person remains. Show that the person remaining is numbered 1.

2. Let $a, a', b, b' \in \mathbb{Z}$ be integers such that $[a]_n = [a']_n$ and $[b]_n = [b']_n$ for some positive integer n. Show that
   (a) ✦ $[a+b]_n = [a'+b']_n$.
   (b) ✦ $[ab]_n = [a'b']_n$.

3. (a) ✦ Compute $\gcd(4567, 58)$, $\gcd(2590, 2018)$, $\gcd(345, 8900)$, $\mathrm{lcm}(91, 252)$, $\mathrm{lcm}(32, 98)$.
   (b) ✦✦ Show that if $a, b \in \mathbb{Z}, a, b > 0$, and $gcd(a, b) = d$, then $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

4. (a) i. ✦✦✦ Let $a = p_1^{r_1} \cdots p_m^{r_m}$ for p_i all distinct primes and $r_i \geq 1$ for all i. Let $b = q_1^{s_1} \cdots q_n^{s_n}$ be another prime factorisation, also with the q_i distinct and $s_i \geq 1$ for all i. (If a or b is one, then let us say that $m = 0$ or $n = 0$, respectively, and we have no prime factorisation.) Prove that $a \mid b$ if and only if for every $i \in \{1, \ldots, m\}$, there exists j with $q_j = p_i$ and $s_j \geq r_i$.
      ii. ✦✦✦ Let $a, b > 1$ have prime power factorizations

$$a = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} q_1^{s_1} \ldots q_l^{s_l}, \quad b = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k} r_1^{t_1} \ldots r_j^{t_j},$$

      with all p_i, q_i, r_i all distinct primes and all exponents positive, but not necessarily having the primes in increasing order. Show that

$$\begin{aligned} gcd(a,b) &= 1 \cdot p_1^{\min(n_1,m_1)} p_2^{\min(n_2,m_2)} \ldots p_k^{\min(n_k,m_k)}, \\ lcm(a,b) &= p_1^{\max(n_1,m_1)} p_2^{\max(n_2,m_2)} \ldots p_k^{\max(n_k,m_k)} q_1^{s_1} \ldots q_l^{s_l} r_1^{t_1} \ldots r_j^{t_j} \end{aligned}$$

      Here we have $1\cdot$ in the first formula so that, if the expression is empty, the answer should be one.
   (b) ✦✦ Let $a, b \in \mathbb{N}$, prove that then $lcm(a, b)gcd(a, b) = ab$.

5. Show that if $a, b \in \mathbb{Z}$ and $a \equiv b \mod n$, then the following holds:
   (a) ✦ For all $c \in \mathbb{Z}, ac \equiv bc \mod n$;
   (b) ✦ For all $c \in \mathbb{Z}, a + c \equiv b + c \mod n$.

   Does either of these statements imply $a \equiv b \mod n$? Which one(s)?

6. (a) ✦✦ Show that if $a, b, k, n \in \mathbb{Z}$, $k > 0$, $n > 0$ and $a \equiv b \mod n$ then $a^k \equiv b^k \mod n$.
   (b) ✦✦✦ Show that if m is an odd integer, then the set

$$A := \{-\frac{m-1}{2}, -\frac{m-3}{2}, \cdots -1, 0, 1, \ldots \frac{m-3}{2}, \frac{m-1}{2}\}$$

   is a complete system of residues modulo m.

7. (a) (✦✦) Let $a, b \in \mathbb{Z}, a, b > 0$, and $d = \gcd(a, b)$. Show that there exists integers s and t such that $as + bt = d$.

   (b) Let $a, b, c \in \mathbb{Z}$, $d = gcd(a, b)$ and consider the equation $ax + by = c$.

      i. (✦✦✦) Show that if $d|c$ and the equation $ax + by = c$ has one integer solution $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$, then it has infinitely many integer solutions.

      ii. (✦) Show that if d does not divide c, then the equation has no solution.

      iii. (✦✦) Conclude that the equation has either infinitely many solutions or no solutions.

8. (a) (✦✦) Let $a, b, n \in \mathbb{Z}$, $n > 0$, $d = gcd(a, b)$. Prove the following statements

      i. (✦✦✦) The equation $ax \equiv b \mod n$ has a solution if and only if $\gcd(a, n)|b$.

      ii. (✦✦) The equation $ax \equiv b \mod n$ has exactly d incongruent solutions if $\gcd(a, n) = d$ and $d|b$.

   (b) (✦✦) Solve the following equations (i.e., give the full set of solutions, which could be empty):

      i. $18x \equiv 30 \mod 42$, $6x \equiv 7 \mod 8$, $3x \equiv 7 \mod 4$.