IA Numbers & Sets – Example Sheet 3

Michaelmas 2025

zoe.wyatt@maths.cam.ac.uk

Questions marked † are more challenging.

1. Solve (i.e. find all solutions of) the equations

   (i) $7x \equiv 77 \mod 40$;

   (ii) $12y \equiv 30 \mod 54$;

   (iii) $3z \equiv 2 \mod 17$ and $4z \equiv 3 \mod 19$.

2. By considering the n fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$ or otherwise, prove that $n = \sum_{d|n} \varphi(d)$.

3. Explain (without electronic assistance) why 23 cannot divide $10^{881} - 1$.

4. Let p be a prime of the form $3k + 2$. Show that if $x^3 \equiv 1 \mod p$, then $x \equiv 1 \mod p$. Deduce that every number is a cube modulo p, that is, $y^3 \equiv a \mod p$ has an integer solution y for all $a \in \mathbb{Z}$.

5. What is the 5th-last digit of $5^{5^{5^{5^5}}}$?

6. Is there a positive integer n for which $n^7 - 77$ is a Fibonacci number?

7. By considering numbers of the form $(2p_1p_2 \ldots p_k)^2 + 1$, prove that there are infinitely many primes of the form $4n + 1$.

8. An RSA encryption scheme (n, e) has modulus $n = 187$ and encoding exponent $e = 7$. Find a suitable decoding exponent d. Check your answer (without electronic assistance) by explicitly encoding the number 35 and then decoding the result.

9. Prove carefully, using the least upper bound axiom, that there is a real number x satisfying $x^3 = 2$. Prove also that such an x must be irrational.

10. Prove that $\sqrt{2} + \sqrt{3}$ is irrational and algebraic.

11. Suppose that $x \in \mathbb{R}$ is a root of a monic integer polynomial, i.e. we have $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0 = 0$, for some integers $a_{n-1}, \ldots, a_0$. Prove that x is either integer or irrational.

12. Show that $\sqrt[100]{\sqrt{3} + \sqrt{2}} + \sqrt[100]{\sqrt{3} - \sqrt{2}}$ is irrational.

13. Let $(x_n)_{n=1}^{\infty}$ and $(y_n)_{n=1}^{\infty}$ be sequences of reals. Show that if $x_n \to 0$ and $y_n \to 0$, then $x_ny_n \to 0$. By considering $x_n - c$ and $y_n - d$, prove carefully that if $x_n \to c$ and $y_n \to d$, then $x_ny_n \to cd$.

14. Let $(x_n)_{n=1}^{\infty}$ be a sequence of reals. Show that if $(x_n)_{n=1}^{\infty}$ is convergent, then we must have $x_n - x_{n-1} \to 0$. If $x_n - x_{n-1} \to 0$, must $(x_n)_{n=1}^{\infty}$ be convergent?

15. † Let n and k be positive integers. Suppose that n is a kth power modulo p for all primes p. Must n be a kth power?