MA3H1 Topics in Number Theory
Example Sheet 3

You should attempt all the questions on this sheet. but questions Q2–Q5 will marked for credit, and must be handed in by **3pm Friday, week 5.**

(1) (i) Practice the Chinese Remainder Theorem: solve the system of simultaneous congruences

$$X \equiv 7 \pmod{13}, \qquad X \equiv 2 \pmod{16}.$$

(ii) Show that the following system of simultaneous congruences does not have a solution

$$X \equiv 3 \pmod{14}, \qquad X \equiv 6 \pmod{26}.$$

(2) With the help of Euler's Theorem, compute

$$2^{3000} \pmod{15}, \qquad 3^{5000} \pmod{31}.$$

(3) (i) Show that if a is odd then $a^2 \equiv 1 \pmod 8$.

(ii) Show that $3^m \equiv 1 \pmod 8$ if and only if m is even.

(iii) Solve the equation $3^m - 2^n = 1$ in non-negative integers m, n.

(4) (i) Find a primitive root modulo p for $p = 5$, 7, 11, 29.

(ii) Let g be a primitive root modulo prime p. Show that g^a is a primitive root modulo p if and only if $\gcd(a, p-1) = 1$.

(iii) How many primitive roots modulo p are there?

(5) **(Wilson's Theorem)** Let p be a prime. Show that $(p-1)! \equiv -1 \pmod p$. **(Hint: use a primitive root.)**

(6) Let $p > 3$ be a prime. Let R (respectively N) be a complete set of quadratic residues (respectively non-residues) modulo p.

(i) Show that

$$\prod_{r \in R} r \equiv -\prod_{n \in N} n \equiv (-1)^{(p+1)/2} \pmod p.$$

(ii) Show that

$$\sum_{r \in R} r \equiv \sum_{n \in N} n \equiv 0 \pmod p.$$

(Hint: use a primitive root.)